



Database and Middleware Automation

Software Version: 10.50.001.000

Linux, Solaris, AIX, and HP-UX

User Guide

Document Release Date: May 2017

Software Release Date: May 2017



Hewlett Packard
Enterprise

Legal Notices

Warranty

The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

Restricted Rights Legend

Confidential computer software. Valid license from Hewlett Packard Enterprise required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Copyright Notice

© 2012-2016 Hewlett Packard Enterprise Development LP

Trademark Notices

Adobe™ is a trademark of Adobe Systems Incorporated.

Microsoft® and Windows® are U.S. registered trademarks of Microsoft Corporation.

UNIX® is a registered trademark of The Open Group.

This product includes an interface of the 'zlib' general purpose compression library, which is Copyright © 1995-2002 Jean-loup Gailly and Mark Adler.

Documentation Updates

To check for recent updates or to verify that you are using the most recent edition of a document, go to: <https://softwaresupport.hpe.com/>.

This site requires that you register for an HP Passport and to sign in. To register for an HP Passport ID, click **Register** on the HPE Software Support site or click **Create an Account** on the HP Passport login page.

You will also receive updated or new editions if you subscribe to the appropriate product support service. Contact your HPE sales representative for details.

Support

Visit the HPE Software Support site at: <https://softwaresupport.hpe.com/>.

Most of the support areas require that you register as an HP Passport user and to sign in. Many also require a support contract. To register for an HP Passport ID, click **Register** on the HPE Support site or click **Create an Account** on the HP Passport login page.

To find more information about access levels, go to: <https://softwaresupport.hpe.com/web/softwaresupport/access-levels>.

HPE Software Solutions Now accesses the HPSW Solution and Integration Portal website. This site enables you to explore HPE Product Solutions to meet your business needs, includes a full list of Integrations between HPE Products, as well as a listing of ITIL Processes. The URL for this website is <https://softwaresupport.hpe.com/km/KM01702731>.

About this PDF Version of Online Help

This document is a PDF version of the online help. This PDF file is provided so you can easily print multiple topics from the help information or read the online help in PDF format. Because this content was originally created to be viewed as online help in a web browser, some topics may not be formatted properly. Some interactive topics may not be present in this PDF version. Those topics can be successfully printed from within the online help.

Contents

Use	23
Accessing DMA	24
Working with workflows	25
The Workflow Execution Architecture	25
Searching for a Workflow	26
Viewing an Existing Workflow	27
Creating a New Workflow	29
Copying a Workflow	32
Exporting a Workflow	33
Importing a Workflow	33
Assigning Roles to a Workflow	33
Viewing the History of a Workflow	34
Sending the History of a Workflow	34
How to send Email of Workflow History and Logs	34
Running a workflow	35
Deleting a Workflow	36
Working with steps	37
Searching for Steps	37
Viewing a Step	37
Creating a New Step	41
Copying a Step	42
Built-in Steps	43
Working with parameters	45
Creating Parameters	46
Assigning Values to Parameters	47
Using Parameters	50
Using Metadata and Policies from a Workflow Step	52
Working with functions	53
Searching for a Function	53
Viewing/Opening a Function	53
Creating a Function	54
Copying a Function	54
Modifying a Function	54
Deleting a Function	55
Working with policies	56
Policy Attribute Types	56
Policy Roles	56

Policy Solution Packs	57
Creating a New Policy	57
Extracting a Policy	57
Determining Where a Policy Is In Use	58
Deleting a Policy	58
Assigning Policies to Roles	59
Scheduling a deployment	60
Deployment Considerations	61
User Considerations	61
Permissions Considerations	61
Timing and Concurrency Considerations	61
Workflows	63
IBM DB2	64
DB2 - Compliance Audit	65
Prerequisites for this Workflow	66
How this Workflow Works	67
How to Run this Workflow	70
Sample Scenarios	73
Parameters for DB2 - Compliance Audit	77
DB2 - Configure HADR Database	78
Prerequisites	79
How this Workflow Works	81
How to Run this Workflow	83
Parameters for DB2 - Configure HADR Database	85
DB2 - Configure Tivoli SAMP on HADR Database	87
Prerequisites	88
How this Workflow Works	89
How to Run this Workflow	91
Parameters for Configure Tivoli SAMP on HADR Database	94
DB2 - Provision Software v2	96
Prerequisites	97
How this Workflow Works	97
How to Run this Workflow	98
Parameters for DB2 - Provision Instance	101
DB2 - Provision Instance	104
Prerequisites	104
How this Workflow Works	105
How to Run this Workflow	106
Parameters for DB2 - Provision Instance	109
DB2 - Provision Database	112
Prerequisites	113
How this Workflow Works	114

How to Run this Workflow	115
Parameters for DB2 - Provision Database	121
DB2 - Patch Fixpack v2	126
Prerequisites	127
Additional requirements	127
How this Workflow Works	128
How to Run this Workflow	129
Parameters for DB2 - Patch Fixpack v2	131
DB2 - Rollback Fixpack v2	132
Prerequisites	133
Additional requirements	134
How this Workflow Works	134
How to Run this Workflow	135
Parameters for DB2 - Rollback Fixpack v2	139
DB2 - Offline HADR Fixpack Parent Flow v3	142
Prerequisites	143
Additional requirements	144
How this Workflow Works	144
How to Run this Workflow	146
Parameters for DB2 - Offline HADR Fixpack Parent Flow	149
DB2 - Offline HADR Apply Fixpack	150
Prerequisites	151
Additional requirements	152
How this Workflow Works	153
How to Run this Workflow	156
Parameters for DB2 - Offline HADR Apply Fixpack	159
DB2 - Offline HADR Rollback Fixpack	161
Prerequisites	162
Additional requirements	163
How this Workflow Works	163
How to Run this Workflow	167
Parameters for DB2 - Offline HADR Rollback Fixpack	170
DB2 - Rollback Helper	172
Prerequisites	172
Additional requirements	173
How this Workflow Works	174
How to Run this Workflow	176
Parameters for DB2 - Rollback Helper	179
DB2 - Fixpack Validator v2	180
Prerequisites	181
Additional requirements	182
How this Workflow Works	182

How to Run this Workflow	184
Parameters for DB2 - Fixpack Validator	186
DB2 - Upgrade Instance and Database	186
Prerequisites	187
How this Workflow Works	188
How to Run this Workflow	190
Parameters for DB2 - Upgrade Instance and Database	194
MySQL	199
MySQL - Compliance Audit	200
Prerequisites for this Workflow	201
How this Workflow Works	202
How to Run this Workflow	204
Sample Scenarios	208
Parameters for MySQL - Compliance Audit	213
MySQL - SQL Release	214
Prerequisites for this Workflow	215
How this Workflow Works	216
How to Run this Workflow	217
Parameters for MySQL - SQL Release	220
MySQL - Upgrade Instance	222
Prerequisites for this Workflow	223
How this Workflow Works	224
How to Run this Workflow	226
Parameters for MySQL - Upgrade Instance	231
MySQL Drop Database	235
Prerequisites for this Workflow	236
How this Workflow Works	237
How to Run this Workflow	238
Parameters for MySQL - Drop Database	239
MySQL - Install Instance	240
Prerequisites for this Workflow	241
How this Workflow Works	242
How to Run this Workflow	243
Parameters for MySQL - Install Instance	245
MySQL - Create Database	246
Prerequisites for this Workflow	247
How this Workflow Works	248
How to Run this Workflow	249
Parameters for MySQL - Create Database	251
MySQL - Start or Stop	252
Prerequisites for this Workflow	253
How this Workflow Works	254

How to Run this Workflow	255
Parameters for MySQL - Start or Stop	257
Oracle	258
Oracle - Compliance Audit v2	260
Prerequisites for this Workflow	261
How this Workflow Works	262
How to Run this Workflow	265
Sample Scenarios	268
Parameters for Oracle - Compliance Audit	272
Patching Database	272
Oracle - Patch Home and Databases v5	275
Prerequisites for this Workflow	277
How this Workflow Works	278
How to Run this Workflow	280
Parameters for Oracle - Patch Home and Databases	281
Oracle - Rollback Patch from Home and Databases v2	283
Prerequisites for this Workflow	284
How this Workflow Works	285
How to Run this Workflow	288
Sample Scenario	291
Parameters for Oracle - Rollback Patch from Home and Databases	293
Apply Oracle Patchset	295
Prerequisites for this Workflow	297
How this Workflow Works	298
How to Run this Workflow	303
Sample Scenario	306
Parameters for Apply Oracle Patchset	307
Clone Oracle Home	311
Prerequisites for this Workflow	312
How this Workflow Works	313
How to Run this Workflow	315
Sample Scenario	317
Parameters for Clone Oracle Home	318
Migrate Oracle Home	320
Prerequisites for this Workflow	321
How this Workflow Works	322
How to Run this Workflow	326
Sample Scenario	328
Parameters for Migrate Oracle Home	330
Oracle - Migrate and Patch Grid Managed Database	331
Prerequisites for this Workflow	333

How this Workflow Works	334
How to Run this Workflow	336
Parameters for Oracle - Migrate and Patch Grid Managed Database	339
The Advanced Database Patching Solution	340
Oracle - Patch Grid Infrastructure and Databases v6	341
Prerequisites for this Workflow	342
How this Workflow Works	343
How to Run this Workflow	346
Sample Scenarios	352
Parameters for Oracle - Patch Grid Infrastructure and Databases v6	357
Oracle - Rollback Patch from Grid Infrastructure and Database	361
Prerequisites for this Workflow	362
How this Workflow Works	363
How to Run this Workflow	366
Sample Scenarios	369
Parameters for Oracle - Rollback Patch from Grid Infrastructure and Database	370
Refreshing Database	371
Oracle - Extract Database via RMAN	373
Prerequisites for this Workflow	374
How this Workflow Works	375
How to Run this Workflow	378
Sample Scenarios	380
Parameters for Oracle - Extract Database via RMAN	382
Oracle - Refresh Database via RMAN	384
Prerequisites for this Workflow	385
How this Workflow Works	386
Sample Scenarios	389
How to Run this Workflow	391
Parameters for Oracle - Refresh Database via RMAN	393
Oracle - Extract and Refresh Database via RMAN	396
Prerequisites for this Workflow	397
How this Workflow Works	398
How to Run this Workflow	402
Sample Scenarios	404
Parameters for Oracle - Extract and Refresh Database via RMAN	408
Oracle - Export Database via Data Pump	410
Prerequisites for this Workflow	411
How this Workflow Works	412

How to Run this Workflow	416
Sample Scenarios	418
Parameters for Oracle - Export Database via Data Pump	423
Oracle - Refresh Database via Data Pump	427
Prerequisites for this Workflow	428
How this Workflow Works	429
How to Run this Workflow	433
Sample Scenarios	435
Parameters for Oracle - Refresh Database via Data Pump	439
Oracle - Migrate Database TTS	444
Prerequisites for this Workflow	446
How this Workflow Works	447
How to Run this Workflow	451
Sample Scenarios	453
Parameters for Oracle - Migrate Database TTS	455
Oracle - Drop Database	456
Prerequisites for this Workflow	457
How this Workflow Works	458
How to Run this Workflow	459
Parameters for Oracle - Drop Database	461
Oracle - Provision Data Guard v6	462
Prerequisites for this Workflow	463
How this Workflow Works	465
How to Run this Workflow	467
Parameters for Oracle - Provision Data Guard	469
Oracle - Create Data Guard Broker Configuration	472
Prerequisites for this Workflow	473
How this Workflow Works	475
How to Run this Workflow	476
Parameters for Oracle - Create Data Guard Broker Configuration	478
Oracle - Configure Data Guard Broker Properties	480
Prerequisites for this Workflow	481
How this Workflow Works	483
How to Run this Workflow	484
Parameters for Oracle - Configure Data Guard Broker Properties	486
Oracle - Data Guard Broker Switchover	488
Prerequisites for this Workflow	489
How this Workflow Works	491
How to Run this Workflow	492
Parameters for Oracle - Data Guard Broker Switchover	494
Parameters for switching the database from primary to standby	494

Parameters for switching the database back from standby to primary	495
Provisioning Grid Infrastructure	495
What Oracle Grid standalone does	496
Oracle - Provision or Upgrade Grid Infrastructure	497
Prerequisites for this Workflow	498
How this Workflow Works	499
How to Run this Workflow	501
Parameters for Oracle - Provision or Upgrade Grid Infrastructure	502
Oracle - Provision Database Software v2	505
Prerequisites for this Workflow	506
How this Workflow Works	507
How to Run this Workflow	509
Parameters for Oracle - Provision Database Software v2	510
Oracle - Provision Database v3	513
Prerequisites for this Workflow	514
How this Workflow Works	515
How to Run this Workflow	518
Parameters for Oracle - Provision Database v3	519
Provisioning RAC	523
What Oracle Grid infrastructure for cluster does	523
Oracle - Provision or Upgrade Grid Infrastructure	524
Prerequisites for this Workflow	525
How this Workflow Works	526
How to Run this Workflow	528
Parameters for Oracle - Provision or Upgrade Grid Infrastructure	530
Oracle - Provision Database Software v2	533
Prerequisites for this Workflow	534
How this Workflow Works	535
How to Run this Workflow	537
Parameters for Oracle - Provision Database Software v2	538
Oracle - Provision Database v3	541
Prerequisites for this Workflow	542
How this Workflow Works	543
How to Run this Workflow	546
Parameters for Oracle - Provision Database v3	547
Oracle - SQL Release v3	551
Prerequisites for this Workflow	554
How this Workflow Works	556
How to Run this Workflow	559

Sample Scenarios	562
Parameters for Oracle - SQL Release v3	566
Microsoft SQL Server	568
MS SQL - Compliance Audit v2	569
Prerequisites for this Workflow	570
How this Workflow Works	571
How to Run this Workflow	573
Sample Scenarios	576
Parameters for MS SQL - Compliance Audit v2	582
MS SQL - Install Patch	583
Prerequisites	583
Process Overview	583
Workflow: MS SQL - Install Patch	584
Solution pack	584
Parameters to expose	585
Input parameters	585
FAQs	587
How do I install the SQL Server patch on all instances on the server?	587
How do I install the SQL Server patch on multiple cluster nodes?	587
MS SQL - Install Cluster Patch	587
Prerequisites	588
Process Overview	588
Workflow: MS SQL - Install Cluster Patch	589
Solution pack	589
Parameters to expose	589
Input parameters	589
FAQs	590
How do I install the SQL Server patch on all instances on the server?	590
How do I install the SQL Server patch on multiple cluster nodes?	591
Refreshing Database	591
MS SQL - Backup Database	592
Prerequisites for this Workflow	593
How this Workflow Works	594
How to Run this Workflow	595
Sample Scenarios	597
Parameters for Backup MS SQL Database	599
MS SQL - Restore Database	602
Prerequisites for this Workflow	604

How this Workflow Works	605
How to Run this Workflow	609
Sample Scenarios	611
Parameters for Restore MS SQL Database	613
MS SQL - Backup and Restore Database	615
Prerequisites for this Workflow	617
How this Workflow Works	618
How to Run this Workflow	621
Sample Scenarios	623
Parameters for Backup and Restore MS SQL Database	627
DB Release for SQL Server v2	631
Prerequisites for this Workflow	634
How this Workflow Works	635
How to Run this Workflow	638
Sample Scenarios	642
Parameters for DB Release for SQL Server v2	645
MS SQL Drop Database v2	648
Prerequisites for this Workflow	649
How this Workflow Works	650
How to Run this Workflow	651
Parameters for MS SQL - Drop Database	653
MS SQL - Upgrade Standalone SQL Instance	653
Prerequisites for this Workflow	654
How this Workflow Works	655
How to Run this Workflow	657
Parameters for MS SQL - Upgrade Standalone SQL Instance	659
MS SQL Rollback Patch	660
Prerequisites for this Workflow	661
How this Workflow Works	662
How to Run this Workflow	664
Parameters for MS SQL Rollback Patch	666
MS SQL - Create AlwaysOn Availability Group v2	667
Prerequisites for this Workflow	668
How this Workflow Works	669
How to Run this Workflow	671
Parameters for MSSQL - Create AlwaysOn Availability Group	673
MS SQL - Install Clustered SQL Instance v2	674
Prerequisites	675
How this workflow works	676
How to run this workflow	677
Parameters for MS SQL - Install Clustered SQL Instance	684
MS SQL - Add Node to Cluster v3	689

Prerequisites	690
How this workflow works	691
How to run this workflow	692
Parameters for MS SQL - Add Node to Cluster	696
MS SQL - Create Database v2	698
Prerequisites	699
How this workflow works	700
How to run this workflow	701
Parameters for MS SQL - Create Database	703
Sybase	706
Sybase - Compliance Audit v2	707
Prerequisites for this Workflow	708
How this Workflow Works	709
How to Run this Workflow	714
Sample Scenarios	718
Parameters for Sybase - Compliance Audit	723
Dump Sybase Database	726
Prerequisites for this Workflow	727
How this Workflow Works	729
How to Run this Workflow	731
Sample Scenarios	733
Parameters for Dump Sybase Database	737
Load Sybase Database Dump	740
Prerequisites for this Workflow	741
How this Workflow Works	743
Sample Scenarios	745
How to Run this Workflow	749
Parameters for Load Sybase Database Dump	751
Dump And Load Sybase Database	754
Prerequisites for this Workflow	756
How this Workflow Works	758
Sample Scenarios	762
How to Run this Workflow	766
Parameters for Dump and Load Sybase Database	769
Sybase - Start or Stop Instance	772
Prerequisites for this Workflow	773
How this Workflow Works	774
How to Run this Workflow	775
Sample Scenario	776
Parameters for Sybase - Start or Stop Instance	777
Sybase Release Management	778
Prerequisites for this Workflow	781

How this Workflow Works	783
How to Run this Workflow	789
Sample Scenarios	792
Parameters for Sybase Release Management	795
Sybase - Patch to Home and Instance	798
Prerequisites for this Workflow	799
How this Workflow Works	800
How to Run this Workflow	806
Sample Scenario	813
Parameters for Sybase - Patch Home and Instance	814
Sybase - Rollback from Home and Instance	822
Prerequisites for this Workflow	823
How this Workflow Works	824
How to Run this Workflow	827
Sample Scenario	832
Parameters for Sybase - Rollback Patch from Home and Instance	834
Provision Sybase ASE 15 Server	836
Prerequisites	837
How this workflow works	838
How to run this workflow	839
Parameters for Provision Sybase ASE 15 Server	844
Configure Sybase ASE 15 Server	848
Prerequisites	848
How this workflow works	850
How to run this workflow	851
Parameters for Configure Sybase ASE 15 Server	853
Create Sybase Database	854
Prerequisites	854
How this workflow works	856
How to run this workflow	856
Parameters for Create Sybase Database	859
Apache Web Server	863
Apache - Provision Software	864
Prerequisites for this workflow	866
How this workflow works	867
How to Run this Workflow	869
Sample Scenarios	872
Parameters for Apache - Provision Software	874
Red Hat JBoss	876
Provision Open Source JBoss 7 StandAlone Mode	877
Prerequisites for this Workflow	878
How this Workflow Works	879

How to Run this Workflow	882
Sample Scenario	884
Parameters for Provision Open Source JBoss 7 StandAlone Mode	885
JBoss - Create and Configure Data Source v2	886
Prerequisites for this Workflow	886
How this Workflow Works	886
How to Run this Workflow	888
Sample Scenarios	890
Parameters for JBoss - Create and Configure Data Source v2	893
JBoss - Code Release v2	895
Prerequisites for this Workflow	895
How this Workflow Works	896
How to Run this Workflow	900
Sample Scenario	903
Parameters for JBoss - Code Release v2	905
JBoss - Provision Software v3	907
Prerequisites for this Workflow	908
How this Workflow Works	909
How to Run this Workflow	912
Sample Scenarios	914
Parameters for JBoss - Provision Software v3	916
JBoss - Patch Software v3	918
Prerequisites for this Workflow	919
How this Workflow Works	920
How to Run this Workflow	922
Sample Scenario	924
Parameters for JBoss - Patch Software v3	925
JBoss - Rollback Patch Software v2	926
Prerequisites for this Workflow	927
How this Workflow Works	928
How to Run this Workflow	930
Sample Scenario	932
Parameters for JBoss - Rollback Patch Software v2	933
Tomcat Application Server	934
Tomcat - Provision Software	935
Prerequisites for this Workflow	937
How this Workflow Works	938
How to Run this Workflow	940
Sample Scenarios	942
Parameters for Tomcat - Provision Software	944
Oracle WebLogic	949

WebLogic - Provision Weblogic Software	950
Prerequisites for this Workflow	952
How this Workflow Works	953
How to Run this Workflow	958
Sample Scenario	961
Parameters for WebLogic - Provision Weblogic Software	965
WebLogic - Provision Weblogic Domain and Admin Server	967
Prerequisites for this Workflow	969
How this Workflow Works	970
How to Run this Workflow	973
Sample Scenario	976
Parameters for WebLogic - Provision Weblogic Domain and Admin Server	980
WebLogic - Provision Advanced Domain and Admin Server	983
Prerequisites for this Workflow	984
How this Workflow Works	985
How to Run this Workflow	989
Sample Scenario	992
Parameters for WebLogic - Provision Advanced Domain and Admin Server	994
WebLogic - Provision Weblogic Managed Servers	996
Prerequisites for this Workflow	998
How this Workflow Works	999
How to Run this Workflow	1002
Sample Scenario	1006
Parameters for WebLogic - Provision Weblogic Managed Servers	1012
Provision WebLogic Cluster	1015
Prerequisites for this Workflow	1017
How this Workflow Works	1018
How to Run this Workflow	1021
Sample Scenario	1023
Parameters for Provision WebLogic Cluster	1025
Increase WebLogic Domain Span	1026
Prerequisites for this Workflow	1028
How this Workflow Works	1029
How to Run this Workflow	1031
Sample Scenario	1034
Parameters for Increase WebLogic Domain Span	1035
WebLogic - Create Trust and Identity Keystore	1037
Prerequisites for this Workflow	1038
How this Workflow Works	1039

How to Run this Workflow	1041
Sample Scenario	1044
Parameters for WebLogic - Create Trust and Identity Keystore ...	1046
WebLogic - Code Release	1047
Prerequisites for this Workflow	1048
How this Workflow Works	1048
How to run this workflow	1052
Sample Scenario	1055
Parameters for WebLogic - Code Release	1058
WebLogic - Create and Configure Datasource	1060
Prerequisites for this Workflow	1061
How this Workflow Works	1062
How to Run this Workflow	1067
Sample Scenario	1070
Parameters for WebLogic - Create and Configure Datasource ...	1078
WebLogic - Patch WebLogic Domain v3	1080
Prerequisites for this Workflow	1081
How this Workflow Works	1082
How to Run this Workflow	1086
Sample Scenario	1089
Parameters for WebLogic - Patch WebLogic Domain V3	1091
WebLogic - Rollback Patch	1093
Prerequisites for this Workflow	1094
How this Workflow Works	1095
How to Run this Workflow	1099
Sample Scenario	1102
Parameters for WebLogic - Rollback Patch	1104
IBM WebSphere	1106
Provision WebSphere and Custom Node	1107
Prerequisites for this Workflow	1108
How this Workflow Works	1110
How to Run this Workflow	1114
Sample Scenario	1118
Parameters for Provision WebSphere and Custom Node	1120
Provision WebSphere Custom Node Profile From Existing Install ..	1124
Prerequisites for this Workflow	1125
How this Workflow Works	1127
How to Run this Workflow	1130
Sample Scenario	1133
Parameters for Provision WebSphere Custom Node Profile From Existing Install	1135
Provision WebSphere and Deployment Manager	1138

Prerequisites for this Workflow	1139
How this Workflow Works	1141
How to Run this Workflow	1146
Sample Scenario	1150
Parameters for Provision WebSphere and Deployment Manager	1152
Provision WebSphere and Stand-Alone	1156
Prerequisites for this Workflow	1157
How this Workflow Works	1159
How to Run this Workflow	1163
Sample Scenario	1167
Parameters for Provision WebSphere and Stand-Alone	1169
Provision WebSphere Stand-Alone Profile From Existing Install	1173
Prerequisites for this Workflow	1174
How this Workflow Works	1176
How to Run this Workflow	1179
Sample Scenario	1182
Parameters for Provision WebSphere Stand-Alone Profile from Existing Install	1184
WebSphere - Provision IBM HTTP Server	1187
Prerequisites for this Workflow	1188
How this Workflow Works	1190
How to Run this Workflow	1196
Sample Scenario	1199
Parameters for WebSphere - Provision IBM HTTP Server	1206
Provision WebSphere 7 and Custom Node	1209
Prerequisites for this Workflow	1210
How this Workflow Works	1211
How to Run this Workflow	1216
Sample Scenario	1220
Parameters for Provision WebSphere 7 and Custom Node	1222
Provision WebSphere 7 and Deployment Manager	1225
Prerequisites for this Workflow	1226
How this Workflow Works	1227
How to Run this Workflow	1232
Sample Scenario	1236
Parameters for Provision WebSphere 7 and Deployment Manager	1238
Provision WebSphere 7 StandAlone Profile	1241
Prerequisites for this Workflow	1242
How this Workflow Works	1243
How to Run this Workflow	1247
Sample Scenario	1251

Parameters for Provision WebSphere 7 StandAlone Profile	1253
Provision IBM HTTP Server 7 and Plug-In	1256
Prerequisites for this Workflow	1257
How this Workflow Works	1258
How to Run this Workflow	1262
Sample Scenario	1267
Parameters for Provision IBM HTTP Server 7 and Plug-in	1271
Create StandAlone from Existing WebSphere 7 Install	1274
Prerequisites for this Workflow	1275
How this Workflow Works	1276
Sample Scenario	1280
How to Run this Workflow	1281
Parameters for Create StandAlone from Existing WebSphere 7 Install	1285
Create Custom Node from Existing WebSphere 7 Install	1289
Prerequisites for this Workflow	1290
How this Workflow Works	1291
Sample Scenario	1294
How to Run this Workflow	1296
Parameters for Create Custom Node from Existing WebSphere 7 Install	1300
Create and Configure WebSphere Data Sources	1303
Prerequisites for this Workflow	1305
How this Workflow Works	1306
How to Run this Workflow	1312
Sample Scenario	1315
Parameters for Create and Configure WebSphere Data Sources	1323
Create and Configure WebSphere Web Server Definitions	1325
Prerequisites for this Workflow	1326
How this Workflow Works	1327
How to Run this Workflow	1331
Sample Scenario	1334
Parameters for Create and Configure WebSphere Web Server Definitions	1338
WebSphere - Code Release	1339
Prerequisites for this Workflow	1340
How this Workflow Works	1341
How to Run this Workflow	1345
Sample Scenario	1351
Parameters for WebSphere - Code Release	1355
WebSphere - Code Release on Cluster	1359
Prerequisites for this Workflow	1359

How this Workflow Works	1360
How to Run this Workflow	1364
Sample Scenario	1366
Parameters for WebSphere - Code Release on Cluster	1370
WebSphere 8 - Patch Network Cell	1374
Prerequisites for this Workflow	1375
How this Workflow Works	1376
How to Run this Workflow	1380
Sample Scenario	1382
Parameters for WebSphere 8 - Patch Network Cell	1383
IBM HTTP Server - Patch Software v2	1383
Prerequisites for this workflow	1385
How this workflow works	1386
How to run this workflow	1390
Parameters for IBM HTTP Server - Patch Software v2	1392
Sample scenario	1393
WebSphere - Provision WebSphere SDK Java	1393
Prerequisites for this workflow	1394
How this workflow works	1395
How to run this workflow	1399
Parameters for WebSphere - Provision WebSphere SDK Java ..	1401
Sample scenario	1402
Configure WebSphere Cluster and Cluster Members	1403
Prerequisites for this Workflow	1405
How this Workflow Works	1406
How to Run this Workflow	1411
Sample Scenario	1414
Parameters for Configure WebSphere Cluster and Cluster Members	1422
WebSphere - Configure IBM HTTP Server	1424
Prerequisites for this Workflow	1425
How this Workflow Works	1426
How to run this workflow	1428
Parameters for WebSphere - Configure IBM HTTP Server	1430
Sample Scenario	1432
IBM HTTP Server - RollBack Patch Software	1436
Prerequisites for this workflow	1437
How this workflow works	1438
How to run this workflow	1442
Parameters for IBM HTTP Server - Rollback Patch Software	1444
WebSphere 8 - Rollback Patch Network Cell	1445
Prerequisites for this Workflow	1446

How this Workflow Works	1447
How to Run this Workflow	1451
Parameters for WebSphere 8 - Patch Network Cell	1453
Promote Solution	1454
Promote Workflow – Export	1455
Prerequisites for this Workflow	1456
How This Workflow Works	1457
How to Run This Workflow	1460
Sample Scenario	1462
Parameters for Promote Workflow – Export	1464
Promote Workflow – Import	1465
Prerequisites for this Workflow	1466
How This Workflow Works	1467
How to Run This Workflow	1472
Sample Scenarios	1476
Parameters for Promote Workflow – Import	1481
Promote Workflow – Export and Import	1483
Prerequisites for this Workflow	1486
How This Workflow Works	1487
How to Run This Workflow	1492
Sample Scenarios	1496
Parameters for Promote Workflow - Export and Import	1502
Discovery	1505
Prerequisites for this Workflow	1507
How this Workflow Works	1508
How to Run this Workflow	1510
Sample Scenarios	1512
Parameters for Discovery	1513
Send documentation feedback	1514

Use

This section provides information about provisioning, patching, installing, and upgrading databases and application servers using workflows.

- ["Accessing DMA" on page 24](#)
- ["Working with workflows" on page 25](#)
- ["Working with steps" on page 37](#)
- ["Working with parameters" on page 45](#)
- ["Working with functions" on page 53](#)
- ["Working with policies" on page 56](#)
- ["Scheduling a deployment" on page 60](#)
- ["Workflows" on page 63](#)

Accessing DMA

To access DMA, open a web browser and specify the following URL:

`https://<HPDMA Server>:8443/dma/login`

Here, *<HPDMA Server>* represents the host name or IP address of your DMA server.

After you have accessed the DMA user interface, enter your user name and password to log in.

After you log in, you can view information about your roles and capabilities by clicking your user name in the upper right corner of the

DMA window.

Working with workflows

A **workflow** is a set of steps used to accomplish a specific operational task or procedure—such as patching a database instance, installing middleware, or auditing all the instances in an organization for compliance with a security standard.

A workflow is deployed to specific targets. There are three types of targets:

- Servers
- Instances
- Databases

DMA targets must be, or in the case of instance and database targets, reside on Server Automation (SA) managed servers. In addition, these servers must have the DMA Client Files policy. See [DMA Client Files Policy](#).

Workflow **steps** contains the actual code used to perform a unit of work detailed in a workflow. A step is typically an executable script, although it can take other forms. Steps are linked together to form the business logic for a task or procedure. You can use a workflow to perform a new business process by building on existing best practices and processes.

Workflow **documentation** should contain information required to understand not only how a procedure is executed, but also how that procedure has been qualified and tested. workflow documentation encapsulates best practices into a shareable document that can be exported for IT auditors, change control boards, or training manuals for new data center administrators.

The Workflow Execution Architecture

DMA controls the flow or progression of a workflow through its component steps. This limits the amount of memory that the DMA client running on the managed server requires.

This procedure explains how DMA runs a workflow:

1. DMA finds the first workflow step to execute.
2. DMA replaces all metadata, parameters, and header variables for this workflow step.
3. The DMA client executes that script and returns the output and errors as it executes.

4. When the script has completed, the DMA client sends the return code back to the DMA server.
5. Based on the value of the return code, DMA decides which workflow step to execute next.
6. DMA repeats step 2 through step 5 until the workflow is completed.

Searching for a Workflow

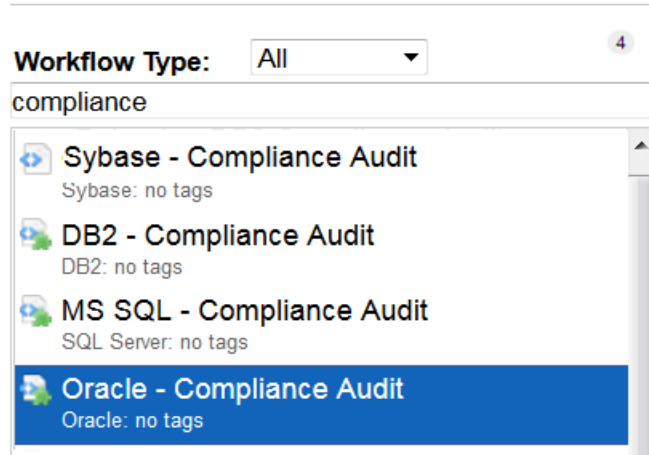
You can use a real-time filter to search for any workflow by name, type, or tags.

In the Workflow Type filter, you can select:

- Other
- OS
- DB2
- MySQL
- Oracle
- PostgreSQL
- SQL Server
- Sybase
- All (default)

Type what you are searching for in the Workflow box, and see the filter results display as you type. The search string is not case-sensitive, as shown in the following figure.

Workflows



Note: The real-time filter feature is available throughout the DMA user interface (UI).

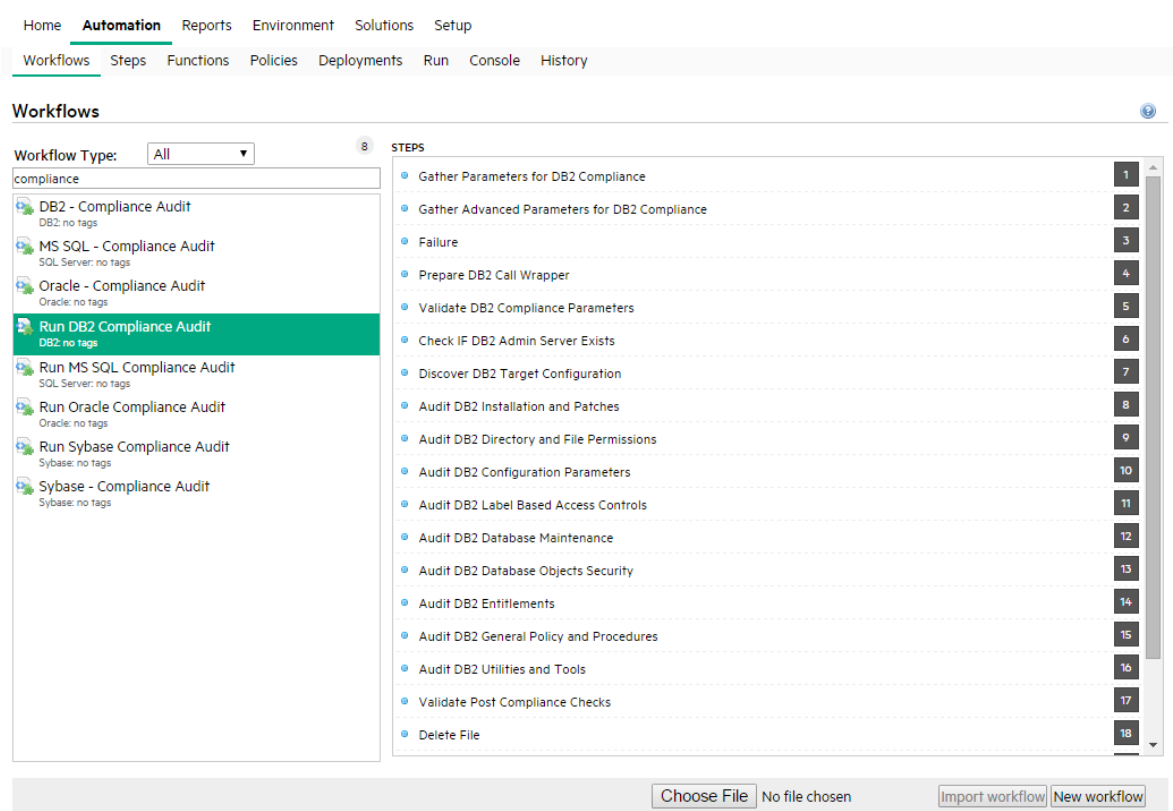
Viewing an Existing Workflow

From the Automation > Workflows page, you can view a list of existing workflows and preview the steps included in any workflow listed.

Steps List

In the Workflows pane, point to the workflow name. As you point to the workflow, you can view the associated steps in the Steps pane:

Example of Steps in a Workflow



Workflow Documentation

In the Workflows pane, click the workflow that you want to view. The Documentation tab opens, as shown in the figure below.

Provided that the workflow is deployable (not locked), you can modify the workflow documentation to suit your environment. To open the documentation editor, click the **Edit** link in the lower right corner.

For formatting information, click the **Help** link in the lower right corner.

The screenshot shows the Oracle Workflow Documentation interface. At the top, there is a navigation bar with links: Home, **Automation**, Reports, Environment, Solutions, and Setup. Below this is a sub-navigation bar with links: Workflows, Steps, Functions, Policies, Deployments, Run, Console, and History. The main heading is "Run Oracle Compliance Audit". Below the heading are tabs: Documentation (selected), Workflow, History, Deployments, and Roles. The Documentation tab displays the following information:

- Name: Run Oracle Compliance Audit
- Tags:
- Type: Oracle
- Target level: Instance

The Documentation section is expanded, showing:

- Purpose**: Audit an Oracle Database instance for compliance with the following Center for Internet Security (CIS) benchmarks and, optionally, compare the audit results to the related PCI and SOX requirements:
 - CIS Security Configuration Benchmark for Oracle Database Server 11g, version 1.1.0, December 2011
 - CIS Security Benchmark for Oracle 9i/10g, version 2.01, April 2005
 - Payment Card Industry (PCI) Data Security Standard Version 2.0, October 2010
 - Sarbanes-Oxley (SOX) Sarbanes-Oxley Act of 2002 Section 302
- Description**: This workflow will audit an Oracle Database instance using CIS Level 1 and Level 2 auditing. It will then compare the results to the pertinent PCI and SOX requirements, where applicable. This audit, which runs in conjunction with the HP DMA reporting tool, can identify more than 175 compliance related problems with an Oracle database. You can view information about the audit on the Console while the audit is running. After the audit has finished, the workflow sends a summary report to each specified email address. You can also view a compliance report on the Reports page.
- Parameters**

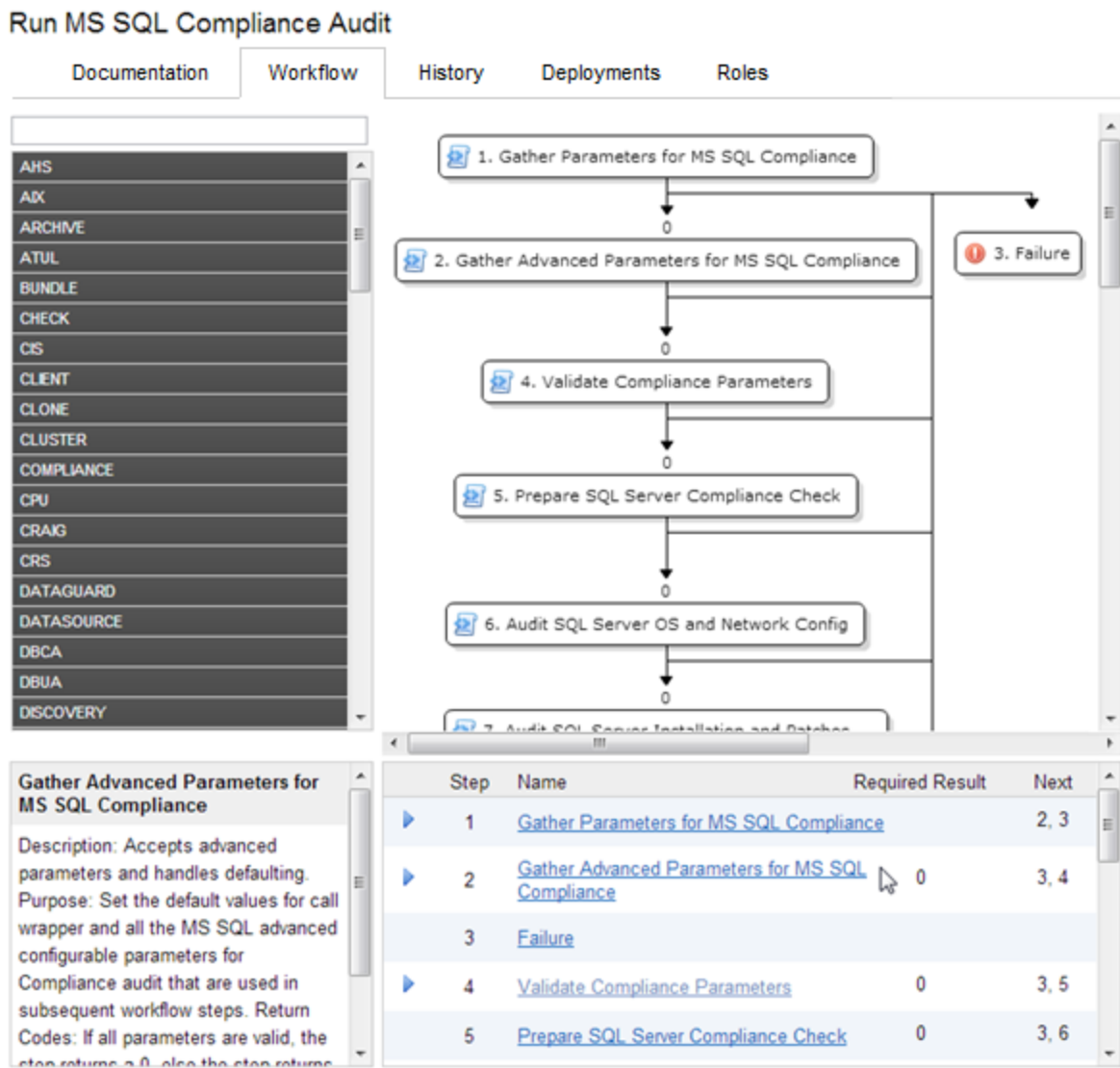
At the bottom of the page, there is a toolbar with buttons: Copy, HIDE, EXPORT, and EXTRACT POLICY. On the right side of the toolbar, there is a link: [HP DMA DATABASE COMPLIANCE SOLUTION PACK](#). A [HELP](#) link is also visible in the bottom right corner of the documentation area.

Workflow Details

From the Documentation tab, click the Workflow tab to view the following information:

A graphical representation of the workflow logic


- A list of all available steps, grouped by tag
- A table listing the steps included in the workflow and the parameters associated with each step .



Creating a New Workflow

To create a new workflow:

1. On the Automation > Workflows page, click **New Workflow**.
The Documentation tab opens.
2. Specify the following information:

- **Name:** A unique name for the workflow.
 - **Tags:** Use this field as a keyword field. Use existing tags or create new ones so that you and others can easily find or filter for this workflow in the future.
 - **Type:** Type of database or middleware software to which this workflow pertains.
 - **Target Level:** This determines which types of targets you can select when you create a deployment. Select Server, Instance, or Database.
 - **Documentation:** Use this field to document the function of this workflow. You will likely develop the workflow documentation in an iterative fashion as you refine the workflow.
3. Add at least one step to your workflow using one or both of the following methods:
- See ["Creating a New Step" below](#)
 - See ["Adding an Existing Step" on the next page](#)
- To delete a step from a workflow, click the "Remove"  button.
4. When you are finished adding and connecting steps, click **Save**.
- "Workflow Saved Successfully" displays in a green bar at the top of the Workflows page.

Creating a New Step

You can use the New Step wizard to create a new step "on the fly" while you are editing a workflow. This is an alternative to creating a step from the Automation > Steps page.

To create a new step by using the New Step wizard:

1. Click the **New Step** link just below the Steps panel. The New Step wizard opens.
2. Specify the information that the wizard prompts you to provide. This will vary depending on the type of step that you are creating (script, email, or variable timer)
3. Click **Next** to advance through the wizard pages.

If you add parameters to your new step, you can specify Plain Text or Password for the parameter type. The value of a Password type parameter is always masked in the DMA user interface.

4. Click **Finish** when you have provided all required information.

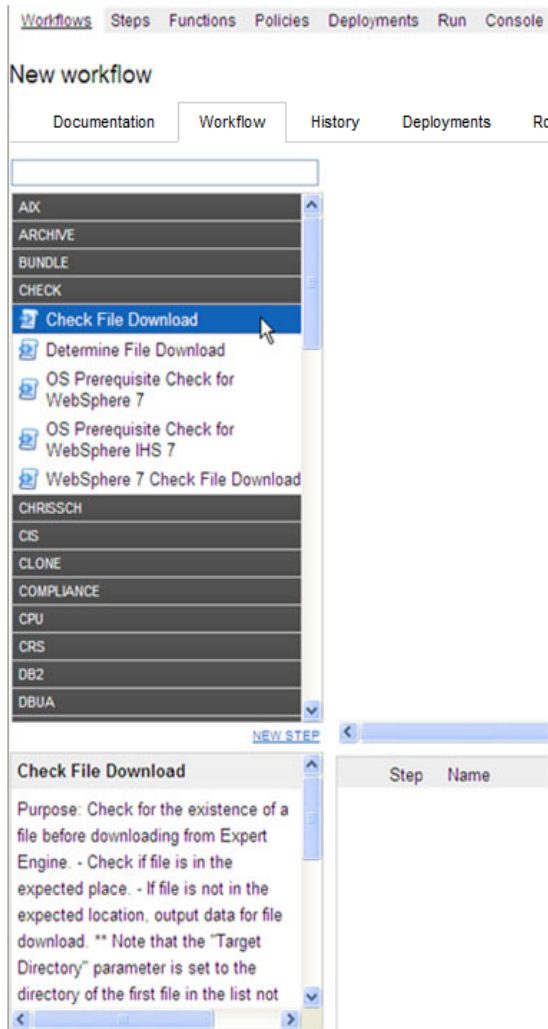
The New Step wizard creates the step and adds it to the workflow after any existing steps.

Adding an Existing Step

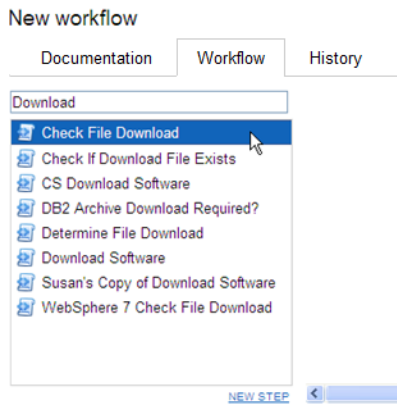
To add an existing step to a workflow, you must first locate the step and then place it in the appropriate spot in the workflow. The following procedure assumes that the workflow has been created, and that you are viewing the workflow tab.

To add an existing step to a workflow:

1. In the steps panel, click one of the tags to show the list of steps that have that tag:



Alternatively, you can type text into the filter box above the Steps panel, and any steps whose names contain that text are listed:



2. Double-click a step to add it to the workflow.
3. In the steps table below the diagram, modify the Required Result and Next values for this step and any pertinent existing steps so that the workflow logic is correct.

Click in the Required Result or Next column to edit the value.

Note: Be sure to always include the built-in SUCCESS and FAILURE steps in your workflows (see ["Built-in Steps" on page 43](#)). Make sure that the final step that the workflow executes is either SUCCESS or FAILURE, depending on the outcome of the previous steps.

Note: A Download Software step is built into your DMA software. This step enables you to download one or more files from the software repository to a specified location on the target server. To locate this step, on the workflow tab, type “download” in the filter box. See ["Download Software" on page 43](#) for additional information.

Copying a Workflow

Copy is available from all the tabs in the Automation > Workflow area. Creating a copy of a workflow saves time by enabling you to reuse information in a workflow by renaming it without having to re-type the workflow’s information.

To make a copy of a workflow:

1. Click **Copy**.

The Documentation tab opens, and the workflow name changes to “Copy of <workflow name>.”

2. Make any changes to the copy.
3. Click **Save**.

Exporting a Workflow

You can export a workflow, and it is saved on the local file system as an SOP file.

When you export a workflow, you export the steps used in that workflow, but you do not export the functions.

To export a Workflow:

1. Go to Automation > Workflows.
2. Click the workflow that you want to export.
3. Click **Export**.
4. A page displays and allows you to select a location to which you want to save the workflow.
5. Click **OK**.
6. Click **Save**.

Importing a Workflow

You can import a workflow that was previously exported as an SOP file.

To import a workflow:

1. On the Automation > Workflows page, click **Browse** to find the workflow you want to import.

Note: In some browsers, this button is labeled Choose File instead of Browse.

2. After you select a file to import, Click **Import workflow**.

Assigning Roles to a Workflow

Roles determine who can read or modify a workflow. You can modify the roles settings for any workflow that you have permission to Write. You can only assign permissions for roles that you have—unless you have a role with Administrator capability.

To assign roles to a workflow:

1. Go to Automation > Workflows.
2. In the Workflows pane, point to the workflow name.
3. Click the workflow you want to view.
The Documentation tab displays.
4. Click the **Roles** tab.
The Roles tab displays.
5. Select or clear the **Read** or **Write** check boxes, depending on the permission you want to grant.
6. Click **Save**.

Viewing the History of a Workflow

Every time that a workflow is saved, a new entry is added to the table on the History tab. The entry shows you when the workflow was saved and by whom it was saved.

Sending the History of a Workflow

You can get the workflow execution history of a workflow by an Email by adding Send Email step to any existing or a new workflow. This step allows to compose an email with a subject and body of the message. The Email can be sent to multiple recipients by providing a list of comma separated Email addresses.

You must install DMA Utility Solution Pack to be able to send an Email of workflow history and logs upon execution of the workflow.

How to send Email of Workflow History and Logs

1. Go to Automation > Steps.
2. Select the Send Email step.
3. Modify the following parameter values as required in the Parameters tab.
 - Body
 - FilePathAndName

- Mailing List
 - Subject
4. Open the workflow for which you have to get history or create a new workflow.
 5. Perform the steps listed in the task [Add an Existing Step](#) to locate and add Send Email step to the workflow.
 6. In the steps table below the workflow diagram, modify the Required Result and Next values for the Send Email step and any pertinent existing steps so that the workflow logic is correct.
 7. Perform the run task to execute the workflow.

On execution of the workflow, an email is sent with the selected information to the specified recipients.

Running a workflow

To “run” a workflow, you specify a deployment and one or more targets. If the deployment contains Runtime specified parameters, they can be entered; otherwise the previously configured parameter values will be displayed.

There are several ways that you can run a workflow:

- From within a workflow or a deployment: After you create, edit, and then save a workflow or a deployment, click the “Would you like to run the workflow now?” link.
- From the Automation > Run page.

To run a workflow from the Run page:

1. Go to Automation > Run.
2. Select a workflow, a deployment, and the target (or targets) where you want to run the workflow.
3. Provide values for any Runtime parameters.

All other parameter values will be displayed for you to review before executing the workflow. It is not possible to change non-Runtime parameter values at this time.

Any workflow with Runtime parameters cannot be scheduled (see ["Scheduling a deployment" on page 60](#)). Workflows with Runtime parameters must be executed manually using Automation > Run.

4. Click **Run Workflow**.
5. Go to the Console or History page to view information about the workflow's progress.

Deleting a Workflow

You can delete a workflow unless its status is “Read Only.” You must either have a role with Administrator capability, or you must have a role that has both Workflow Creator capability and permission to Write the workflow.

Caution: If you delete a workflow that has associated deployments, the associated deployments will be deleted automatically with the workflow.

To delete a workflow:

1. Go to Automation > Workflows.
2. Open the workflow you want to delete.
3. Click and confirm delete.

Working with steps

Steps are reusable automation components. They are assembled into workflows that automate a task or system healing action. steps can accept input parameters for customization and provide output for subsequent steps to use.

Searching for Steps

Steps are reusable automation components. They are assembled into workflows that automate a task or system healing action. steps can accept input parameters for customization and provide output for subsequent steps to use.

Viewing a Step

Note: Steps provided by are Read Only. You must copy a step before you can modify it. See ["Copying a Step" on page 42](#).

To view information about a specific step:

1. Go to Automation > Steps.

You can also access individual steps from the Steps tab on the Solutions page or the list of steps associated with a workflow.

2. In the Steps pane, point to the step name that you want to view.

As you point to a step, the workflows that use that particular step is shown in the Workflows pane.

3. Click the step you want to view.

There are seven tabs that you can use to view information about this step:

- ["General Tab" on the next page](#)
- ["Action Tab" on the next page](#)
- ["Parameters Tab" on page 40](#)
- ["History Tab" on page 40](#)

- ["Workflows Tab" on page 41](#)
- ["Solutions Tab" on page 41](#)
- ["Roles Tab" on page 41](#)

Note: To modify the properties of a step, you must have Write permission for that step (see ["Roles Tab" on page 41](#) and [Roles, Capabilities, and Permissions](#)).

General Tab

The General tab displays information about a step. In the Properties area, you can view and edit the following information:

- **Name:** Step's name (must be unique).
- **Tags:** Use this field as a keyword field to type descriptive words about a step's function, language, compliance, etc., so that you can easily find or filter for this step.
- **Type:** Determines where or at what level a step is executed.
- **Category:** Specifies the type of step. There are three step categories:
 - **Script:** Executes the code on the Action tab.
 - **Email:** Sends an email to the specified email address.
 - **Variable Timer:** Waits the number of minutes that you specify before the workflow proceeds to the next step. This is useful, for example, if you want to allow time for the system to reboot.

The Category setting determines which options are available on the Action tab.

You can only specify the Category field when you are creating a new step. You cannot edit the Category field after a step has been saved.

In the Documentation area, you can view or edit documentation that is related to the step.

Action Tab

The Action tab enables you to view and specify the action that a step takes when that step is used in a workflow. The options available on the Action tab reflect the Category type specified on the General tab.

Actions for Script Type Steps

For a Script type step, you must specify two items:

- **Call wrapper** – the location of the interpreter that executes the script.

Specify `jython` here to run the script using DMA's built-in python interpreter.

You can specify a different call wrapper if you prefer. For example:

```
/bin/ksh
```

```
/usr/bin/perl
```

```
powershell -ExecutionPolicy unrestricted -File, cscript /E VBS
```

Caution: If you install Windows PowerShell on a managed server, and you want to use it as an DMA call wrapper, you must restart the SA agent on that server. To do this, restart the Opsware Agent service.

- **Code** – the script to run using the Call wrapper.

You can type or paste the script into the Code box, or you can use the Import Script tool.

The Import Script tool replaces any information in the Code field with the contents of a file that you specify. To import a script, follow these steps:

- Click the **Import Script** link.
- Click **Browse** to locate the script you want to import.
- Click **Open** to import the script (or click **X** to cancel).

Actions for Email Type Steps

For an Email type step, you must specify three things:

- **To** – email address to which the email message will be sent.
- **Subject** – subject of the email message.
- **Message** – content (body) of the email message. The message can be in either of the two formats - plain text or HTML. If the message is in HTML format, it must have an opening tag (`<html>`) and a closing tag (`</html>`).

Note: If the message in HTML format contains bold, italics, or underlined text, the text should be preformatted using the `<pre>` tag to keep the formatting intact.

Actions for Variable Timer Type Steps

For a Variable Timer type step, you must specify one option: the Delay. This is the number of minutes that you want the workflow to wait before executing the next step.

Parameters Tab

Parameters enable you to pass information into or out of a step. You set the input to a value, and the output parameter is set within the code (see ["Working with parameters" on page 45](#)). Script steps can have both input and output parameters. All other step types can only have input parameters.

- Input Parameters

The Parameters tab defines the variables that a workflow sets when running a step so that the step can run against different objects and still be reusable. For example, in a database backup, the directory where the backup should be placed would be a good candidate for an input parameter so that both development and production database backups could use the step without modification.

- Output Parameters

Script type steps enable you to define output parameters as well as input parameters. Steps use output parameters to provide information to be used by downstream steps. For example, if a step determines the location of the Oracle Home directory on a target server, it can add that location to its set of output parameters for subsequent steps to use.

Note: If you want to remove a parameter from a step, you can click the Remove link for that parameter. If that parameter is associated with a workflow, however, you cannot remove it, and the Remove link is not available.

History Tab

Every time that a step is saved, a new entry is added to the table on the History tab. The entry shows you when the step was saved and by whom it was saved. If you click an entry in the table, the action information for that version of the step is displayed in the Details area.

Workflows Tab

The Workflows tab shows you a list of the workflows that use this step. If you have permission to Read a specific workflow, you can view or edit information pertaining to that workflow by clicking its name.

Solutions Tab

The Solution tab shows you a list of the Solution Packs that include this step. To view information about a particular Solution Pack, click the name of that Solution Pack. For more information, see [Solutions](#).

Roles Tab

The Roles tab shows you which user groups have Write permission for the step.

Permissions settings for baseline steps (steps that are shipped with DMA) cannot be changed, even by an DMA Administrator. To change permissions for any other step, select or clear the check boxes to grant or revoke Write access.

If there is a “—” in the Write column, none of the roles have Write access to the step. For more information on changing permissions as an DMA Administrator, see [Permission Settings](#).

Creating a New Step

You do not need any special permissions to create new steps. To use your new step in a workflow, however, you must have Write permission for that workflow (see [Roles, Capabilities, and Permissions](#)).

To create a new step:

1. Go to Automation > Steps.
2. Click **New Step**.
3. Specify the following information on the General tab:
 - Name: Unique name of the step.
 - Tags: Use this field as a keyword field, to type descriptive words about a step's function,

language, compliance, etc. so that you can easily find or filter for this step.

- **Type:** Helps you decide where or at what level to run a step.
 - **Category:** Specifies the type of step.
4. Specify the information required on the Action tab:
 - For a Script type step, specify the Call wrapper and Code (see ["Actions for Script Type Steps" on page 39](#)).
 - For an Email type step, specify the email address, subject, and content (see ["Actions for Email Type Steps" on page 39](#)).
 - For a Variable Timer type step, specify the Delay (see ["Actions for Variable Timer Type Steps" on page 40](#)).
 5. *Optional:* In the Documentation area, add documentation that describes the step that you are creating—for example: describe its purpose, dependencies, parameters, and return codes.
 6. *Optional:* Specify any parameters that this step uses (see ["Parameters Tab" on page 40](#)).
 7. *Optional:* Specify who is allowed to modify this step (see ["Roles Tab" on the previous page](#)).
 8. Click **Save**.

Copying a Step

Since steps provided by are read-only, you must first copy a step before you can modify it. You do not need any special permissions in order to copy a step. To use your copied step in a workflow, however, you must have Write permission for that workflow (see [Roles, Capabilities, and Permissions](#)).

To copy an existing step:

1. Go to Automation > Steps.
2. Click a step that you want to modify.
3. Click **Copy**.
4. Specify a unique name for the copy.
5. Modify the step to suit your objective.
6. Click **Save** in the lower right corner.

Built-in Steps

There are three utility steps that are provided with your DMA software:

- ["Success" below](#)
- ["Failure" below](#)
- ["Download Software" below](#)

You can use these steps to build workflows.

Note: It is good practice to always include a SUCCESS step and a FAILURE step in your workflows. The final step that a workflow executes should be either SUCCESS or FAILURE, depending on the return code of the previous step.

Success

This step is intended to be used as the terminal step in a workflow when the workflow has successfully executed the previous steps. A workflow may contain multiple Success steps depending on its branching logic. After the Success step executes, the Console and History pages indicate that the workflow execution status is SUCCESS.

Failure

This step is intended to be used as the terminal step in a workflow when a step in the workflow has failed. Typically, there will only be one Failure step in the Workflow—but you can have multiple Failure steps, depending on the workflow's branching logic. After the Failure step executes, the Console and History pages indicate that the workflow execution status is FAILURE.

Download Software

This step enables you to conveniently transfer a group of files from the software repository to a target server. This is useful, for example, when you are using an DMA workflow to install software on one or more target servers.

This step has the following parameters:

Table: Download Software Parameters

Parameter	Type	Required	Description
FileNames	input	yes	Comma-delimited list of files to download.
TargetDir	input	yes	Directory on the target server where the files will be downloaded.
Download Files	output	n/a	Comma-delimited list of files.

You must specify both input parameters. You can use the output parameter in downstream workflow steps.

This step has the following dependencies:

- You must first add any files that will be transferred to the software repository. See [Importing a File into the Software Repository](#) for instructions.
- File names must be unique. When referencing files in this step's FileNames input parameter, specify a comma-separated list of the uploaded file names.

Note that it is important to specify the actual file names, and not the SA package names.

This Step has the following return codes:

Table: Download Software Return Codes

Return Code	Meaning
0	All files were successfully downloaded.
1	A fatal error occurred while files were being downloaded.
9	One or more files were successfully downloaded.output.

Working with parameters

You create parameters at the step level, and then you assign values at either the workflow level or the deployment level. The following topics provide examples that illustrate how parameters are created and then used at various levels.

- ["Creating Parameters" on the next page](#)
- ["Assigning Values to Parameters" on page 47](#)
- ["Using Parameters" on page 50](#)

The following figure shows an example of a step whose purpose is to validate all the input parameters required for the workflow. This step provides output parameters that are consumed by the subsequent steps in the workflow.

Note: Password type parameters are masked throughout the DMA user interface.

Figure: Automation > Steps > Parameters Tab

Automation > Steps > Parameters Tab

Parse Oracle Inventory

General Action **Parameters** History Workflows Solutions Roles

Parameters

INPUT PARAMETERS ADD

- Inventory Files ✗
- Oracle Account** ✗
- Oracle Home ✗
- Server Wrapper ✗

OUTPUT PARAMETERS ADD

- CRS Account ✗
- CRS Active Version ✗
- CRS Group ✗
- CRS Home ✗
- CRS Home Name ✗
- CRS Nodes ✗
- Cluster Nodes ✗
- Inventory Groups ✗
- Inventory Locations ✗

✗ Parameter is in use and cannot be removed.

Type: Plain Text

Name: Oracle Account

Default Value:

Description: Optional: Oracle user that will own the Oracle Home. This is required only if inventory does not exist.

Copy

Creating Parameters

You can add, modify, and remove parameters for any step for which you have Write permission (see [Roles, Capabilities, and Permissions](#)).

To create a new parameter:

1. Go to Automation > Steps.
2. Select the step that you want to modify (or create a new step).
3. Go to the Parameters tab.
4. Use the Add link to add a new input or output parameter. Specify the following information:

- Type: Plain Text or Password.
- Name: A unique name (within this step) for the parameter.
- Value: The default value of this parameter.

The default value is encrypted before it is stored in the DMA database.

The value of Password type parameters are always masked in the DMA user interface.

- Description: Information that indicates the purpose of this parameter and how its value should be specified. For example:

Required: Unique node name that cannot contain any of the following special characters / \ * , : ; = + ? | < > & % ' " [] > # \$ ^ { }. If you plan to federate into an existing cell later, make sure that the node name is unique within that cell.

5. Click **Save**.

Assigning Values to Parameters

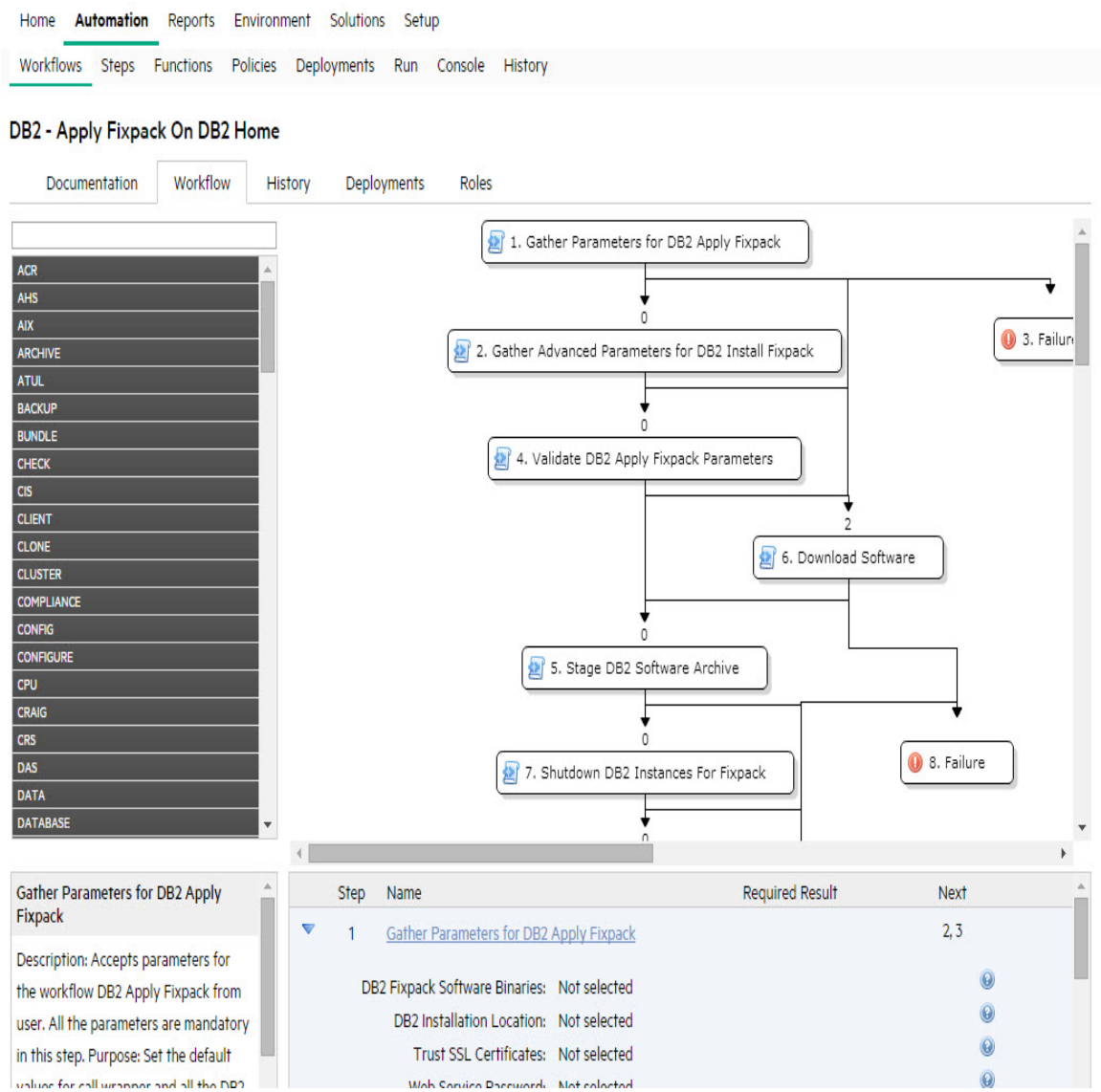
Parameters are defined in steps, but their values are assigned at the workflow level, the deployment level, or with a run action.

Parameters whose values are assigned at the workflow level typically either have constant values or values that are determined at execution time using custom fields. For example, a parameter's value may change based on the organization. In this case, the parameter remains consistent, but the value assigned to that parameter changes.

To assign parameter values at the workflow level, go to the Automation > Workflows > Workflow tab.

Once you go to the Workflow tab, view the workflow table located below the workflow diagram. If the step contains an input parameter, there is an arrow next to each step that, when clicked, displays the "values" that can be associated with that step's parameters.

Figure: Workflow Tab with Step Parameters Displayed



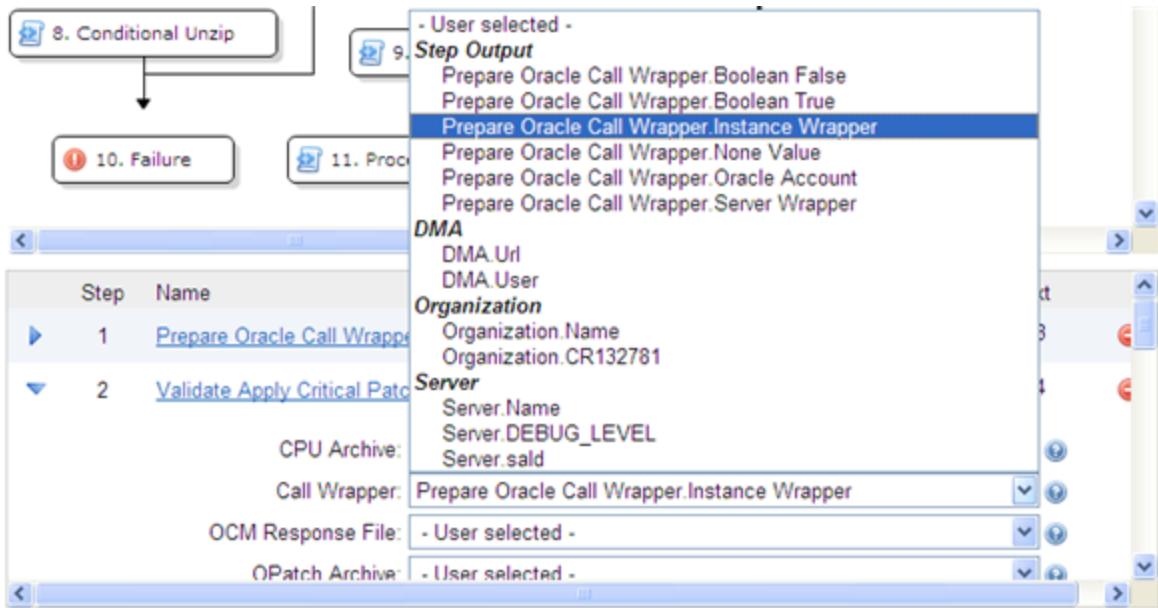
Note: When you are working with parameters at the deployment level or with a run action the parameters are not as static as parameters that you would set at the workflow level. If you know that you have a value that changes often, do not assign it at the workflow level—assign it, instead, at the deployment level. For more information, see ["Using Parameters" on page 50](#).

The drop-down list associated with each input parameter contains built-in metadata and any user-defined Custom Fields.

If a prior step in the workflow contains an output parameter, that output parameter will be included in the drop-down list for that parameter.

In the following figure, for example, the output parameters of the Gather Parameters for MS SQL Compliance step are available to provide values for the input parameters of the Validate Compliance Parameters step. The DMA, organization, and server metadata items are also available.

Figure: Automation > Workflow Tab: Parameter “Values” Drop-Down List



If you assign an output parameter from a previous step to an input parameter at the workflow level, that input parameter does not appear in the deployment parameters list. All parameters that are not either assigned to a Custom Field or mapped at the workflow level will be modifiable at the deployment level. Any parameter that is not set in the workflow or at the deployment level will use the default value assigned for that step.

Assigning Values to Parameters at the Workflow Level

To assign values to parameters at the workflow level:

1. Go to Automation > Workflows.
2. Perform one of the following tasks:
 - Click **New Workflow** to create a workflow.
 - Select an existing editable workflow.
3. Go to the Workflow tab.

The steps in the workflow display in the workflow table, below the workflow diagram. The arrows to the left of each step expand that step to display any parameters associated with the step. If a step has no input parameters, the arrow does not appear.

- A numeric value in the Required Result column is the return code that must be received from at least one parent node in order for that step to run.
 - You can use the Next field to reorder your workflow's steps
4. Click the arrow next to each step. The input or output parameter "values" display in a drop-down list. Assign a value from the "Values" list (as shown in Figure: Automation > Workflow Tab: Parameter "Values" Drop-Down List) to the desired parameter.
 5. Click **Save**.

The Workflow page opens, and the following message displays: "Workflow saved successfully. Would you like to deploy the workflow now?"

To proceed, see [Deployments](#).

Using Parameters

There are three points at which you can assign parameter values: in the workflow, in the deployment, and at run time.

Parameter values should be assigned at the deployment level when the value is specific to the targets that are part of the deployment. For example, you may wish to use the same workflow with production and development servers, but you need to use a different parameter value for each environment. This can be accomplished by creating one deployment of that workflow for production servers, and a second deployment for development servers. This allows you to set the same parameter differently for the each set of targets.

Note: If you assign a value to a parameter at the workflow level, that parameter does not display at the deployment level, so it cannot be overridden.

In a deployment, you can specify parameter values using static text, built-in custom fields, user-defined custom fields, and policy attributes. You will not see any output parameters from other steps on the Deployment page, however; mapping output to input parameters is only possible in the Workflow editor.

If you create a Deployment and then add parameters to your Step, any newly-created parameters appear in the Deployment parameter list and contain the default value assigned in the Step editor.

To assign parameter values at the deployment level:

1. Perform one of the following actions:
 - Click the ... **Would you like to deploy the workflow now** link at the top of the page (this is available immediately after you save a workflow).
 - Create new deployment (see [Creating a New Deployment](#)).
2. On the Targets tab, specify the following:
 - Name: Type a unique deployment name
 - Workflow: If you clicked the link in step 1, the workflow name is pre-populated. If you are creating a new deployment, select a workflow from the list.

Click **View Workflow** if you need to see the workflow for which you are creating a deployment.

 - Schedule (optional): Select a deployment schedule from the drop-down list (see ["Scheduling a deployment" on page 60](#)).

Note: On the Deployments > Parameters tab, if you select Runtime and try to save a deployment with a schedule, you cannot save until you clear the check box or unschedule the deployment.

3. Add the targets from the available pool.
4. Go to the Parameters tab.
5. For each parameter whose value you want to specify, follow these steps:

- a. Select the source of the parameter value from the drop-down list on the far right:

Inventory Files: Optional: Comma-separated list of fully-qualified Oracle inventory files. If this parameter is not specified, the workflow looks for the oraInst.loc file in /etc and /var/opt/oracle.

Custom Field ▼
 Fixed Value
 Custom Field
 Policy Attribute
 Runtime Value

- b. If you selected Fixed Value, Custom Field, or Policy Attribute, specify the parameter value in the text box.

– If you selected Custom Field or Policy Attribute, select a custom field or policy attribute from the drop-down list.

– If you selected Fixed Value, simply type the value in the text box.

– If you selected Runtime, the text box is disabled. You will specify the parameter value at run time.

To replace all parameter values with their default values assigned at the step level, click **Restore Defaults**.

6. Click **Save**.

The Deployment page opens, and the message “Deployment saved successfully. Would you like to run the workflow now?” displays. For more information, see ["Running a workflow" on page 35](#).

Using Metadata and Policies from a Workflow Step

You can use metadata from any workflow step type by using the `${Object.Attribute}` syntax.

For example, the `${Instance.Password}` metadata variable would be replaced at run-time with the actual password for the instance on which this workflow step was executed.

For example, if the password for a given instance were password, the script

```
var password = "${Instance.Password}"
```

would be replaced with

```
var password = "password"
```

at run time.

You can also replace user-defined metadata using these conventions.

Working with functions

Functions are reusable pieces of code that can be included in automation steps. Any common routine or operation that multiple steps perform is a good candidate for a function. Functions can be tagged with keywords indicating the language in which they are written and the operating system with which they work.

DMA now supports Python-style imports for functions. If your function has the “python” or “jython” tag, and a step attempts to import it using standard Python syntax (for example: `import ostools`), DMA will now facilitate that import.

Previously, functions were “injected” into the step code just prior to step execution. This mechanism is still available so that existing automation content can be used. Python-style imports are now the preferred method for importing functions, however.

Note that DMA functions can import other functions.

Searching for a Function

You can use a real-time filter to locate a function by name or by tags. Type what you are searching for in the Functions field, and the filter results will display as you type.

Viewing/Opening a Function

From the Automation > Functions page, you can view all existing functions as well as preview a function's code.

To view or modify a particular function, select its name in the Functions list. Detailed information about that function is then displayed. The Code tab shows you the code that implements that function. The Steps and Functions tabs show you which steps and other functions, respectively, use that function.

Note: Some functions are read-only.

Creating a Function

To create a function:

1. Go to Automation > Functions.
2. Click **New function**. The General tab opens.
3. Specify a unique Name for the function.
4. *Optional:* Specify any Tags or Documentation in the appropriate areas.

When adding a new DMA python function module, you must add a tag "python" or "jython" if the module needs to import other modules. Adding the tag "python" or "jython" will ensure that the dependent function modules are downloaded and that the DMA GUI displays the dependent function modules correctly.

5. Click the **Code** tab.
6. Type or paste new code in the Code area.
7. Click **Save**.

Note: Functions must contain script code. You cannot save a function without script code.

Copying a Function

To copy a function:

1. Go to Automation > Functions.
2. Select a function.
3. Click **Copy**.
4. Type a new name for function.
5. Click **Save**.

Modifying a Function

Before you modify a function, make sure that no workflows that use this function are running. If a workflow uses a function in multiple steps, and that function is modified after the workflow starts

running, the function will be different in later steps than it was in earlier steps. This is because the function is imported just prior to step execution.

To modify a function:

1. Go to Automation > Functions.
2. Select the function that you want to modify.
3. Edit the desired information.
4. Click **Save**.

Note: You cannot modify read-only functions.

Deleting a Function

Because functions are imported at run time, it is possible to delete a function that is used by steps or other functions—this would break those steps or functions. DMA does not check to determine whether a function is being used before deleting it.

To delete a function:

1. Go to Automation > Functions
2. Select the function to delete.
3. Click and confirm delete.

Note: You cannot delete read-only functions.

Working with policies

Policies are reusable sets of attributes that can be used as parameter values in deployments. Deployments can reference policy attributes to change the automation behavior. Policies provide values for input parameters. They can contain fixed values or reference Custom Fields.

Policies enable DMA to manage groups of hundreds or thousands of servers at a time without the need to configure each individual server. For example, you could create a Web Server Policy that defines what every web server in your data center looks like. This policy might contain the following attributes:

- Software List
- Root Password
- Apache User ID
- Apache User Password

The Software List attribute would be a list of software that must be installed on every web server. This might include openssl, apache, perl, etc.

Policy Attribute Types

Policies have three different types of attributes:

- Text: This is a simple text value that users can view while deploying and running automation.
- Password: This is a simple text value. However, the value is masked (obfuscated) when displayed so that users cannot see the value.
- List: This is a free-form text field that can contain comma-delimited lists of values or other large text data not suitable for a Text type attribute.

Policy Roles

When you create a policy, you can specify which users and user groups are allowed to Read or Write that policy. Read permission enables the user who is deploying a workflow to access the policy attributes when specifying parameter values. Write permission enables the user to modify the policy.

Policy Solution Packs

Certain DMA solution packs include Policies. You can modify the attributes values for these Policies, but you cannot add or remove attributes. You can, however, make a copy of a solution pack Policy and then customize that copy.

Creating a New Policy

You can create and use Policies to provide values for various Deployment scenarios.

To create a new policy:

1. Go to Automation > Policies.
2. Click **New Policy**.
3. Type a unique Name for your policy.
4. In the Attributes area, perform the following actions for each attribute you want to add:
 - a. Specify a unique name (within the policy).
 - b. From the drop-down list, select this attribute's type: Text, List, or Password. See "[Policy Attribute Types](#)" on the previous page for details.
 - c. Click **Add**.
 - d. Specify the value of the attribute
 - e. *Optional:* On the Roles tab, select the Read box for any users or user groups that you want to be able to use this policy to provide parameter values in a deployment. Select the Write box for any users or groups that you want to be able to modify this policy (add or remove attributes).
5. Click **Save**.

Extracting a Policy

You can automatically create a reusable policy that provides values for all input parameters associated with a workflow. This is a convenient way to create a policy.

To extract a policy:

1. Go to Automation > Workflows.
2. Select the workflow that you want to work with.
3. Click the **Extract Policy** link at the bottom of the page.
4. Specify values for each attribute listed.
5. *Optional:* Add any new attributes that you want to use.
6. *Optional:* Remove any attributes that you do not want to use.
7. *Optional:* On the Roles tab, select the Read box for any users or user groups that you want to be able to use this policy to provide parameter values in a deployment. Select the Write box for any users or groups that you want to be able to modify this policy (add or remove attributes).
8. Click **Save**.

Determining Where a Policy Is In Use

To determine where a policy is in use:

1. Go to Automation > Policies.
2. Select a policy.
3. Click the **Deployments** tab to see where the policy is in use.

Deleting a Policy

To delete a policy:

1. Go to Automation > Policies.
2. Select a policy.
3. Click the **Deployments** tab to see where the policy is in use. You cannot delete a policy if it is being used. If the policy is being used, follow these steps for each deployment listed:
 - a. Select the deployment.
 - b. Click the **Parameters** tab.

- c. Change any parameter values that reference this policy so that this policy is no longer referenced by the deployment.

The Delete button on the Policy page will be activated after you disassociate the policy from all deployments.

4. Click **Delete** in the lower left corner of the Policy page.

Assigning Policies to Roles

To change permissions for a policy, select (or clear) the check boxes to grant (or revoke) Read and Write access. For more information on changing permissions as an administrator, see [Permission Settings](#)

To assign a policy to a role:

1. Go to Automation > Policies.
2. In the Policies pane, click the policy that you want to view. The Attributes tab displays.
3. Click the **Roles** tab.
4. Select or clear the Read or Write check boxes as appropriate.
5. Click **Save**.

Scheduling a deployment

DMA enables you to schedule a deployment. This is useful, for example, if you want the Discovery workflow to run periodically in your environment (see [Discovery](#)).

You can use one of the following pre-defined schedules, or you can specify a custom schedule.

Schedule	When the Workflow Runs
None	When you click Run .
Every hour	Every hour at the top of the hour (for example: 06:00, 07:00, 08:00, and so on).
Twice a day	Every day at 11:15 and 23:15 UTC.
Once a day	Every day at 2:45 UTC.

Custom schedules are specified using standard cron expressions. For example, the following custom schedule would run the Workflow at 11:45 PM Coordinated Universal Time (UTC— also known as Greenwich Mean Time, or GMT) every Saturday:

Custom Schedule

Minutes (0-59):

45

Hours (0-23):

23

Days of month (1-31):

*

Months (1-12):

*

Weekdays (sun-sat or 0-6):

6

Set schedule

The following instructions show you how to schedule an existing deployment. You can also schedule a deployment as you create it.

To schedule a deployment:

1. Go to Automation > Deployments.
2. In the Workflows column, select the workflow associated with the deployment that you want to schedule.
3. In the Deployments column, select the deployment that you want to schedule.
4. From the Schedule drop-down menu, do one of the following things:

- Select one of the pre-defined schedules described above.
 - Select Custom, and specify the schedule using a `cron` expression.
5. Click **Save**.

Deployment Considerations

Deployments with Runtime parameter values cannot be scheduled. If a Smart Group is associated with a scheduled deployment, that Smart Group will be evaluated each time that this deployment runs (see [Smart Groups](#)). If the schedule is removed from an existing deployment, any workflows that are running as part of a previously scheduled deployment will finish, but no new ones will start until a new schedule is set.

User Considerations

A scheduled deployment is run by the user who most recently saved that deployment. This user name is displayed on the Automation > Console and Automation > History pages.

Permissions Considerations

You must have permission to Read, Write, and Execute a deployment in order to schedule it.

In a scheduled deployment, the workflow is run by the user who most recently modified the deployment. If that user's Run permission is revoked after the deployment is scheduled, the deployment will not run—although it will continue to be scheduled, and a log message will be generated at each scheduled run time.

Timing and Concurrency Considerations

All schedules use the DMA server local time zone.

When a workflow runs as part of a scheduled deployment, a separate “job” is created for each target server, instance, and database—and a separate line appears on the Console and History pages. These

separate jobs run concurrently. This is the same behavior that occurs if the deployment is run manually.

If the workflow takes longer to run on a given target (server, instance, or database) than the interval between deployments, scheduled deployments for that target will be skipped. If the scheduled deployment runs the workflow on multiple targets, DMA will skip only those targets where the workflow is still running.

If a scheduled deployment for a target is skipped, a job is created for that target but the workflow does not actually run. The job will show that the deployment for that target was skipped because another workflow was still running.

There is no limit on the number of scheduled deployments. Too many deployments executing simultaneously, however, can cause performance problems.

In a multiple DMA server implementation, only one DMA server will run the scheduled deployment—which DMA server actually runs the deployment is non-deterministic.

Workflows

This section provides information regarding workflows used in DMA.

- ["IBM DB2" on page 64](#)
- ["Microsoft SQL Server" on page 568](#)
- ["MySQL" on page 199](#)
- ["Oracle" on page 258](#)
- ["Sybase" on page 706](#)
- ["Apache Web Server" on page 863](#)
- ["Red Hat JBoss" on page 876](#)
- ["Oracle WebLogic" on page 949](#)
- ["IBM WebSphere" on page 1106](#)
- ["Tomcat Application Server" on page 934](#)
- ["Promote Solution" on page 1454](#)

Note: The documentation contains workflows, steps, and parameters that are referred to by their base names. The names in the DMA user interface may have a version appended, for example, v2 or v3.

IBM DB2

Workflow type	Workflow name
Compliance	"DB2 - Compliance Audit" on the next page
HADR	"DB2 - Configure HADR Database" on page 78
	"DB2 - Configure Tivoli SAMP on HADR Database" on page 87
	"DB2 - Offline HADR Fixpack Parent Flow v3" on page 142
	"DB2 - Offline HADR Apply Fixpack" on page 150
	"DB2 - Offline HADR Rollback Fixpack" on page 161
Provisioning	"DB2 - Provision Software v2" on page 96
	"DB2 - Provision Instance" on page 104
	"DB2 - Provision Database" on page 112
	DB2 - Deinstall installation
Patching Patching	"DB2 - Patch Fixpack v2" on page 126
	"DB2 - Rollback Fixpack v2" on page 132
Upgrading	"DB2 - Upgrade Instance and Database" on page 186

DB2 - Compliance Audit

The "DB2 - Compliance Audit" workflow enables you to audit a IBM DB2 LUW instance for compliance with the following security benchmark requirements:

- Center for Internet Security (CIS) security configuration benchmarks for DB2 Database Server 8, 9, 9.5 version 1.1.0, December 2009
- Payment Card Industry (PCI) data security standard version 2.0, October 2010
- Sarbanes-Oxley (SOX) requirements Sarbanes-Oxley Act of 2002 Section 302

The workflow performs CIS Level 1 and Level 2 auditing and identifies compliance related problems with a DB2 instance.

The workflow performs the checks included in the CIS benchmark and then maps those CIS checks to the benchmark type that you specify in the Compliance Type parameter. The audit summary email will match the Compliance Type that you specify.

Although this workflow runs at the database level, the compliance report is generated only at the DB2 instance level; hence, in such cases, if the same workflow runs for another database created on the same DB2 instance, then there will be redundant results in the instance level compliance check report.

To use this workflow in your environment, see the following information:

Topic	Information Included
"Prerequisites for this Workflow"	List of prerequisites that must be satisfied before you can run this workflow
"How this Workflow Works"	Information about what the workflow does, including validation checks performed, steps executed, and step descriptions
"How to Run this Workflow"	Instructions for running this workflow in your environment
"Sample Scenarios"	Examples of typical parameter values for this workflow
Parameters	List of input parameters for this workflow

Prerequisites for this Workflow

Be sure that the following prerequisites are satisfied before you run the "DB2 - Compliance Audit" workflow:

- The latest DMA solution packs require the latest DMA platform. To use the latest solution packs, update the DMA platform. DMA10.20 solution packs are supported on DMA10.20 (and later).
- You have installed the Database Compliance solution pack.

The workflow, which by default runs against a DB2 database, requires the following:

- The user (typically root) has unchallenged `sudo` access and can access all required files and directories.
- The DB2 instance and database must exist on the target machine, and the user running the workflow must have sufficient privileges to run the required DB2 commands and queries against the DB2 system table on the target machine.
- Login credentials must be stored in metadata.
- Certain DB2 feature compliance checks require a DB2 license (as recommended by IBM) to ensure that the workflow runs.
- DB2 Admin Server related checks are performed only if the Admin server is found on the target DB2 machine (it may have been attached to any DB2 Instance). There cannot be more than one DB2 Admin Server on the target machine.

How this Workflow Works

This workflow performs the following actions:

- Prepares to run the workflow by gathering information about the target DB2 instance and validating parameter values.
- Audits the various configuration settings specified in the pertinent CIS, SOX, or PCI benchmark.
- Composes and sends an email containing the results of the audit.

Note: The emails are sent through the mail server configured on the DMA server. You can configure the mail server in the path below:

DMA setup > Configuration > Outgoing Mail > Server.

Validation Checks Performed

This workflow validates the following conditions:

1. Any Excluded Checks specified by the user refer to actual CIS, SOX, or PCI benchmark checks.
 - a. Any email addresses specified are valid addresses.
2. The workflow can create the temporary file that will store the compliance check results.

Steps Executed

The "DB2 - Compliance Audit" workflow includes the following steps. Each step must complete successfully before the next step can start. If a step fails, the workflow reports a failure and all subsequent steps are skipped.

Steps Used by Run DB2 Compliance Audit

Workflow Step	Description
Gather Parameters for DB2 Compliance	This step sets the default values for all the DB2 configurable parameters used in the compliance audit and in subsequent workflow steps.
Gather Advanced Parameters for DB2 Compliance	This step sets the default values all the DB2 advanced configurable parameters used in the compliance audit and in subsequent workflow steps.
Prepare DB2 Call Wrapper	This step constructs the commands that will be used to execute subsequent workflow steps as either the OS administrative user (root) or the owner of the DB2 instance.
Validate DB2 Compliance	This step accepts input and default parameters and validates them for the DB2 database.

Steps Used by Run DB2 Compliance Audit, continued

Workflow Step	Description
Parameters	
Check if DB2 Admin Server Exists	This step verifies that there is a DB2 Admin Server on the target machine. If the DAS name is found, then a string is returned with the name.
Discover DB2 Target Configuration	This step discovers any DB2 configurations that have been set up on the target server and uses that information to run the workflow.
Audit DB2 Installation and Patches	This step audits the recommendations in Section 1, Installation and Patches, of the Center for Internet Security (CIS) Configuration Benchmarks for DB2.
Audit DB2 Directory and File Permissions	This step audits the recommendations in Section 2.x, DB2 Directory and File Permissions, of the Center for Internet Security (CIS) Configuration Benchmarks for DB2.
Audit DB2 Configuration Parameters	This step audits the recommendations in Sec 3.x.x, DB2 Configurations, of the Center for Internet Security (CIS) Configuration Benchmarks for DB2.
Audit DB2 Label Based Access Controls	This step audits the recommendations in Section 4.x, Auditing and Logging, of the Center for Internet Security (CIS) Security Configuration Benchmarks for DB2.
Audit DB2 Database Maintenance	This step audits the recommendations in Section 5.x, Database Maintenance, of the Center for Internet Security (CIS) Configuration Benchmarks recommendations for DB2.
Audit DB2 Database Objects Security	This step audits the recommendations in Section 6.x, Securing Database Objects, of the Center for Internet Security (CIS) Security Configuration Benchmarks for DB2.
Audit DB2 Entitlements	This step audits the recommendations in Section 7.x, Entitlements, of the Center for Internet Security (CIS) Security Configuration Benchmarks for DB2.
Audit DB2 General Policy and Procedures	This step audits the recommendations in Section 8.x, General Policy and Procedures, of the Center for Internet Security (CIS) Security Configuration Benchmarks for DB2.
Audit DB2 Utilities and Tools	This step audits the recommendations in Section 9.x, DB2 Utilities and Tools, of the Center of Internet Security (CIS) Configuration Benchmarks for DB2.
Validate Post-Compliance Checks	This step reads the temporary file that contains the results of the compliance audit and prints the audit results to the DMA Console. If email addresses were specified, then it also creates a report in HTML format that will be emailed to those addresses by a later step in the workflow.
Send Compliance Email	This step sends the previously generated compliance audit report to the specified email addresses.

Steps Used by Run DB2 Compliance Audit, continued

Workflow Step	Description
Delete File	This step deletes the specified file on the target server.

How to Run this Workflow

The following instructions show you how to customize and run the ["DB2 - Compliance Audit"](#) workflow in your environment.

For detailed instructions to run DMA workflows—using the Oracle - Compliance Audit workflow as an example—see DMA Quick Start Tutorial.

The workflow provides default values for some parameters. These default values are usually sufficient for a "typical" installation. You can override the defaults by specifying parameter values in the deployment. You can also expose additional parameters in the workflow, if necessary, to accomplish more advanced scenarios. Any parameters not explicitly specified in the deployment will have the default values listed in [Parameters for DB2 - Compliance Audit](#).

Note: Before following this procedure, review the ["Prerequisites for this Workflow"](#), and ensure that all requirements are satisfied.

To use the Run DB2 Compliance Audit workflow:

1. Create a deployable copy of the workflow.
2. Determine the values that you will specify for the following parameters:

Parameters Defined in this Step: Gather Parameters for DB2 Compliance

Parameter Name	Default Value	Required	Description
Compliance Type	CIS	optional	Type of compliance report that will be generated by the workflow. Supported types are: CIS = Center for Internet Security (CIS) Security Configuration Benchmark PCI = Payment Card Industry (PCI) Data Security Standard SOX = Sarbanes-Oxley (SOX) sections 302.2, 302.4b, 302.4c, and 302.5 requirements
DB2 Latest Fixpack Number	no default	required	The latest DB2 UDB Fixpack Number for the specific DB2 version against which the DB2 Compliance workflow is running.
Excluded Compliance Checks	no default	optional	Comma-separated list of compliance checks to exclude from the audit. For example: 1.2, 2, 3.*, 5*, 6.1.2 Make sure that the checks specified here correspond with the compliance audit type (CIS, PCI, or SOX) that you are running.

Parameters Defined in this Step: Gather Advanced Parameters for DB2 Compliance

Parameter Name	Default Value	Required	Description
Email Addresses to Receive Report	no default	optional	The email address (or multiple email addresses separated by commas without spaces) to which the compliance test results are sent.

Note: This is the minimum set of parameters required to run this workflow. You may need to expose additional parameters depending on your objectives.

3. In the workflow editor, expose any additional parameters that you need. You will specify values for those parameters when you create the deployment.
4. Save the changes to the workflow (click **Save** in the lower right corner).
5. Create a new deployment.
6. On the Parameters tab, specify values for the required parameters listed in step 2 and any additional parameters that you have exposed. You do not need to specify values for those parameters whose default values are appropriate for your environment.
7. On the Targets tab, specify one or more targets for this deployment.
8. Save the deployment (click **Save** in the lower right corner).
9. Run the workflow using this deployment.

To verify the results:

The workflow will complete and report SUCCESS on the Console if it has run successfully. If an error occurs during workflow execution, the error is logged, and the workflow terminates in the FAILURE state.

Information about each compliance check is displayed in the step output on the Console (and the History page) for each of the audit steps.

A summary of the compliance audit is also displayed in the step output for the Validate Post Compliance Checks step.

To view the reports:

A compliance audit summary in HTML format is emailed to all parties on the Email Addresses to Receive Report list.

After you run this workflow, you can generate two types of compliance reports on the Reports page:

- Database Compliance Report
- Database Compliance Detail Report

To access the Database Compliance reports:

1. Go to the Reports page.
2. At the bottom of the page, specify the following settings:

For the Database Compliance Report:

- a. Select the Database Compliance report.
- b. Select the organization where your target resides.
- c. Because this report lists the latest compliance audit reports for all targets in the specified organization, you do not specify a Server, Database, or Time span.

For the Database Compliance Detail Report:

- a. Select the Database Compliance Details report.
- b. Select the organization where your target resides.
- c. Specify the Server and Instance that you selected when you created your deployment.

3. Click **Run report**.

Sample Scenarios

This topic shows you how to use various parameters to achieve the following compliance audit scenarios in your environment using the "DB2 - Compliance Audit" workflow.

Scenario 1: Perform a Partial CIS Compliance Audit and Email the Results

In the scenario, the following checks are excluded from the audit:

- Section 7: Entitlements
- Section 9: DB2 Utilities and Tools

A summary report is sent to the three parties listed in the Email Addresses to Receive Report parameter.

Parameter Name	Example Value	Description
Compliance Type	CIS	Type of compliance report that will be generated by the workflow. Supported types are: CIS = Center for Internet Security (CIS) Security Configuration Benchmark PCI = Payment Card Industry (PCI) Data Security Standard SOX = Sarbanes-Oxley (SOX) sections 302.2, 302.4b, 302.4c, and 302.5 requirements
DB2 Latest Fixpack Number	8	The latest DB2 UDB Fixpack Number for the specific DB2 version against which the DB2 Compliance workflow is running.
Excluded Compliance Checks	7.*,9.*	Comma-separated list of compliance checks to exclude from the audit. For example: 1.2, 2, 3.*, 5*, 6.1.2 Note: Make sure that the checks specified here correspond with the compliance audit type (CIS, PCI, or SOX) that you are running.
Email Addresses to Receive Report	DB2DBAdminTeam@mycompany.com, DB2DBAdminMgr@mycompany.com, CustomerSupportTeam@mycompany.com	Comma-separated list of email addresses for those individuals or groups who will receive a copy of the compliance audit report.

Note: Some of these parameters are not exposed by default in the deployment.

Be sure that the default values for all remaining input parameters are appropriate for your environment.

Scenario 2: Perform a Full PCI Compliance Audit and Email the Results

A summary report is sent to the three parties listed in the Email Addresses to Receive Report parameter.

Parameter Name	Example Value	Description
Compliance Type	PCI	Type of compliance report that will be generated by the workflow. Supported types are: CIS = Center for Internet Security (CIS) Security Configuration Benchmark PCI = Payment Card Industry (PCI) Data Security Standard SOX = Sarbanes-Oxley (SOX) sections 302.2, 302.4b, 302.4c, and 302.5 requirements
DB2 Latest Fixpack Number	8	The latest DB2 UDB Fixpack Number for the specific DB2 version against which the DB2 Compliance workflow is running.
Email Addresses to Receive Report	DB2DBAdminTeam@mycompany.com, DB2DBAdminMgr@mycompany.com, CustomerSupportTeam@mycompany.com	Comma-separated list of email addresses for those individuals or groups who will receive a copy of the compliance audit report.

Note: Some of these parameters are not exposed by default in the deployment.

Be sure that the default values for all remaining input parameters are appropriate for your environment.

Scenario 3: Perform a Full SOX Compliance Audit and Email the Results

A summary report is sent to the three parties listed in the Email Addresses to Receive Report parameter.

Parameter Name	Example Value	Description
Compliance Type	SOX	Type of compliance report that will be generated by the workflow. Supported types are: CIS = Center for Internet Security (CIS) Security Configuration Benchmark PCI = Payment Card Industry (PCI) Data Security Standard SOX = Sarbanes-Oxley (SOX) sections 302.2, 302.4b, 302.4c, and 302.5 requirements
DB2 Latest Fixpack Number	8	The latest DB2 UDB Fixpack Number for the specific DB2 version against which the DB2 Compliance workflow is running.
Email Addresses to Receive Report	DB2DBAdminTeam@mycompany.com, DB2DBAdminMgr@mycompany.com, CustomerSupportTeam@mycompany.com	Comma-separated list of email addresses for those individuals or groups who will receive a copy of the compliance audit report.

Note: Some of these parameters are not exposed by default in the deployment.

Be sure that the default values for all remaining input parameters are appropriate for your environment.

Scenario 4: Perform a Full CIS Compliance Audit and Display the Results on the DMA Console

In the scenario, all scorable checks are performed, and the compliance audit report is displayed only on the DMA Console. In this case, a summary report is not emailed. This scenario would be appropriate for initial testing.

It is not necessary to specify any input parameters in this scenario unless the DB2 inventory file is located in a non-standard directory.

Parameter Name	Example Value	Description
Compliance Type	CIS	Type of compliance report that will be generated by the workflow. Supported types are: CIS = Center for Internet Security (CIS) Security Configuration Benchmark PCI = Payment Card Industry (PCI) Data Security Standard SOX = Sarbanes-Oxley (SOX) sections 302.2, 302.4b, 302.4c, and 302.5 requirements

Note: Some of these parameters are not exposed by default in the deployment.

Be sure that the default values for all remaining input parameters are appropriate for your environment.

Parameters for DB2 - Compliance Audit

The following tables describe the required and optional input parameters for this workflow. Some of these parameters are not initially visible in a deployment. For most parameters, if you do not specify a value for a parameter, a default value is assigned

For information about which steps use which parameters, see ["How this Workflow Works"](#).

Parameters Defined in this Step: Gather Parameters for DB2 Compliance

Parameter Name	Default Value	Required	Description
Compliance Type	CIS	optional	Type of compliance report that will be generated by the workflow. Supported types are: CIS = Center for Internet Security (CIS) Security Configuration Benchmark PCI = Payment Card Industry (PCI) Data Security Standard SOX = Sarbanes-Oxley (SOX) sections 302.2, 302.4b, 302.4c, and 302.5 requirements
DB2 Latest Fixpack Number	no default	required	The latest DB2 UDB Fixpack Number for the specific DB2 version against which the DB2 Compliance workflow is running.
Excluded Checks	no default	optional	Comma-separated list of compliance checks to exclude from the audit. For example: 1.2, 2, 3.*, 5*, 6.1.2 Note: Make sure that the checks specified here correspond with the compliance audit type (CIS, PCI, or SOX) that you are running.

Parameters Defined in this Step: Gather Advanced Parameters for DB2 Compliance

Parameter Name	Default Value	Required	Description
Email Addresses to Receive Report	no default	optional	The email address (or multiple email addresses separated by commas without spaces) to which the compliance test results are

Parameters Defined in this Step: Gather Advanced Parameters for DB2 Compliance, continued

Parameter Name	Default Value	Required	Description
			sent.
Latest Patch	no default	optional	The latest DB2 UDB Fixpack Number for the specific DB2 version against which the DB2 Compliance workflow is running.

DB2 - Configure HADR Database

This workflow configures IBM DB2 High Availability Disaster Recovery (HADR) on the existing DB2 setup.

This workflow configures DB2 database(s) for IBM DB2 LUW (Linux, UNIX, and Windows) on the target source and destination servers where this workflow is deployed. It currently supports DB2 versions 10.1 and 10.5 on Red Hat Linux and AIX servers. This is an instance level workflow. It validates that DB2 installations exist on primary node and standby node and that they have the prerequisites. It configures the database with the HADR feature. This workflow is supported on Red Hat Enterprise Linux and AIX operating system platforms.

This workflow supports the following:

1. To generate the default primary and standby HADR database configuration and to configure HADR.
2. To deploy a user specified golden template of the DB2 HADR database configuration on the primary and to use a default standby configuration for HADR.
3. To deploy a user specified golden template of the DB2 HADR database configuration on the standby and to use a default primary configuration for HADR.
4. To use a user specified golden template of the primary and standby HADR database configuration for HADR.

To use this workflow in your environment, see the following information:

Topic	Information Included
"Prerequisites" below	List of prerequisites that must be satisfied before you can run this workflow
"How this Workflow Works" on page 81	Information about what the workflow does, including validation checks performed, steps executed, and step descriptions
"How to Run this Workflow" on page 83	Instructions for running this workflow in your environment
"Parameters for DB2 - Configure HADR Database" on page 85	List of input parameters for this workflow

Prerequisites

Before performing the procedures in this section, your environment must meet the following minimum requirements:

- SSH service must be turned on for both primary and standby host computers.
- The source and destination host computer is configured with SSH password-less login across the nodes (primary to standby and vice versa).
- A TCP/IP interface must be available between the HADR host computers, and a high-speed, high-capacity network is recommended.
- Use identical host computers for the HADR primary and standby databases. That is, they should be from the same vendor and have the same architecture.
- Both the primary and standby host computers must run one of the following operating systems (that is supported by IBM DB2 10.1 or 10.5 and DMA):
 - Linux
 - AIX

See the DMA *Support Matrix* for specific operating system versions, available at:

<https://softwaresupport.hpe.com/>.

- The operating system on the primary and standby host computer must be the same version, including patches.
- DB2 software must be provisioned on both the primary and standby host computer.

Tip: You can use DB2 - Provision Software workflow to accomplish this.

- The DB2 instance must be provisioned on both primary and standby host computer.

Tip: You can use DB2 - Provision Instance workflow to accomplish this.

- The DB2 database must be created on the instance at the primary host computer on which the workflow will be deployed.
- **Tip:** You can use DB2 - Provision Database workflow to accomplish this.
- DB2 instance on primary host computer must be up and running on both the primary and standby host computer.
- Installation media:

The DB2 server installation software binary file from IBM.

Installation software binary file must be available locally or available for download from the software repository.

- Storage:

4-6 GB to provision the DB2 software.

1 GB for each DB2 instance.

1 GB for each DB2 database (more may be required for your configuration).

At least 1 GB for Catalog tablespace.

If automatic storage is on, 1 GB on the default directory where the default tablespace will be created.

- Unchallenged ability to become the DB2 database user.
- The operating system kernel parameters and shared memory is properly configured.
- License for DMA.
- License for DB2 Database version 9.5, 9.7, 10.1, or 10.5.

Note: You have 90 days before you are required to purchase a DB2 license.

- The following workflow requirements:

Workflow	Requirements
DB2 - Configure HADR Database	<p>The sudo package is installed on the target servers.</p> <p>The target servers have the gunzip and tar utilities in the environment path.</p>

Refer to the [IBM Documentation](#) for the following:

- Complete installation and infrastructure requirements for IBM DB2.
- Acceptable types and range of values when using DMA advanced parameters to configure IBM DB2 HADR settings.

How this Workflow Works

This workflow performs the following actions:

Configures IBM DB2 HADR on the existing DB2 setup.

Steps Executed

The DB2 - Configure HADR Database workflow includes the following steps. Each step must complete successfully before the next step can start. If a step fails, the workflow reports a failure and all subsequent steps are skipped.

Steps Used by DB2 - Configure HADR Database

Workflow Step	Description
Gather DB2 Source and Destination Instances	This step gathers data on DB2 source and destination HADR instances.
Gather Parameters for Configure DB2 HADR	This step accepts mandatory parameters for the workflow.
Gather Advanced Parameters for Configure DB2 HADR	This step accepts optional parameters for the workflow.
Validate DB2 Compliance Parameters	This step prepares the call wrappers (server, instance) level as needed to become the owner of the DB2 Server or Instance owner user and perform the appropriate task as necessary.
Validate Parameters for Configure DB2 HADR On Primary Node	This step validates all the input parameter values received in the gather and advanced gather input parameter steps, validate the DB2 target and make sure it meets all the necessary criteria to setup the HADR Database on the given targets.
Download Software	This step automates the transfer of files from the SA Software Library to individual managed servers for use in downstream workflow steps. Verifies checksum of each file transferred.
Configure DB2 HADR Network Service Port On Primary Node	This step checks for unused DB2 HADR port and service on primary cluster node and sets it based on user input values.
Configure DB2 HADR Database On Primary Node	This step prepares the database configuration and deploys on the primary cluster node instance database to enable HADR feature.

Steps Used by DB2 - Configure HADR Database , continued

Workflow Step	Description
Backup DB2 HADR Database On Primary Node	This step sets up the database on archive log mode and takes backup of the database.
Stop DB2 Instance	This step stops the DB2 HADR instance.
Restart DB2 Instance	This step restarts the DB2 HADR instance.
Backup Online DB2 HADR Database On Primary Node	This step takes the online backup for the database at primary cluster node instance database.
Transfer DB2 HADR Database Backup To Standby Node	This step transfers the online database backup file from primary cluster node to standby cluster node.
Configure DB2 HADR Service Network Port On Standby Node	This step checks for unused DB2 HADR port and service on standby cluster node and sets it based on user input values.
Cleanup On Failure For Standby Node	This step checks for unused DB2 HADR port and service on standby cluster node and sets it based on user input values.
Restore DB2 HADR Database On Standby Node	This step restores online database backup taken at the primary cluster node and brings up the database.
Configure DB2 HADR Database On Standby Node	This step prepares the database configuration and deploys on the standby cluster node instance database to enable HADR feature.
Startup DB2 HADR Service on Standby Node	This step runs the DB2 command to activate/startup the HADR service on database.
Cleanup On Failure For Primary Node	This step cleans up the HADR service port and database configuration files from primary cluster node machine.
Verify DB2 HADR Service On Primary Node	This step verifies if the HADR service is up and running on primary node of HADR database.
Discover DB2 Databases	This step audits the server's physical environment looking for DB2 databases.

Results Verification

- The workflow uses the IBM utility “db2pd -d <database name> -hadr” and runs it on the primary and standby nodes. It verifies the results by parsing the resultset and looks up for the specific parameter values to confirm that the HADR setup is complete and it is up and running.

- Run the "db2 "takeover hadr on database <HADR Database Name>" command on the standby node machine as an instance user. This performs the failover test and verifies that the takeover was performed and it switches the standby to primary and the primary to standby database.
- The workflow runs Discovery and updates the instance(s) and databases(s) information in DMA database for future reference.

How to Run this Workflow

The following instructions show you how to customize and run the DB2 - Configure HADR Database workflow in your environment.

Tip: For detailed instructions to run DMA workflows, see *DMA Quick Start Tutorial*.

The workflow provides default values for some parameters. These default values are usually sufficient for a "typical" installation. You can override the defaults by specifying parameter values in the deployment. You can also expose additional parameters in the workflow, if necessary, to accomplish more advanced scenarios. Any parameters not explicitly specified in the deployment will have the default values listed in ["Parameters for DB2 - Configure HADR Database" on page 85](#).

Note: Before following this procedure, review the ["Prerequisites" on page 79](#), and ensure that all requirements are satisfied.

To use the DB2 - Configure HADR Database workflow:

1. Create a deployable copy of the workflow (see "Create a Deployable Workflow" in *DMA Quick Start Tutorial*)

- a. Determine the values that you will specify for the following parameters.

Parameters Defined in this Step: Gather DB2 Source and Destination Instances

Parameter Name	Example Value	Description
DB2 Destination HADR Instance	hadr105 [aixom02.mycompany.com]	The standby node instance name of the remote server. Administration tools, such as the DB2 Control Center, use this parameter to contact the remote server. In the bridge execution workflow, this instance will be used at the run time to run the specific steps configured to run on the standby instance node. The value will be set at the run time.
DB2 Source HADR Instance	hadr105 [aixom01.mycompany.com]	The primary node instance name of the local server. Administration tools, such as the DB2 Control Center, use this parameter to contact the local server. In the bridge execution workflow, this instance will be used at the run time to run the specific steps configured to run on the primary instance node. The value will be set at the run time.

Parameters Defined in this Step: Gather Parameters for Configure DB2 HADR

Parameter Name	Example Value	Description
DB2 HADR Database Name	DB2_HADR	The database name for which the High Availability Disaster Recovery will be configured. The database name must be available on the primary instance node.
DB2 HADR Local Service Name	DB2_HADR_SERVICE_P1	This parameter specifies the TCP service name for which the local high availability disaster recovery (HADR) process accepts.
DB2 HADR Port Number	58234	This parameter specifies the TCP service port number for which the high availability disaster recovery (HADR) process accepts connections. The same port will be used in the primary and standby node for HADR communication.
DB2 HADR Remote Instance Name	hadr105	This parameter specifies the instance name of the remote server. Administration tools, such as the DB2 Control Center, use this parameter to contact the remote server. High availability disaster recovery (HADR) also checks whether a remote database requesting a connection belongs to the declared remote instance.
DB2	DB2_HADR_SERVICE_	This parameter specifies the TCP service name

Parameters Defined in this Step: Gather Parameters for Configure DB2 HADR, continued

Parameter Name	Example Value	Description
HADR Remote Service Name	P1	for which the remote high availability disaster recovery (HADR) process accepts connections.
DB2 HADR Standby Host Name	aixom2.mycompany.com	This parameter specifies the TCP/IP host name or IP address of the remote high availability disaster recovery (HADR) database server.

2. In the workflow editor, expose any additional parameters that you need. You will specify values for those parameters when you create the deployment or at runtime.
3. Save the changes to the workflow (click **Save** in the lower right corner).
4. Create a new deployment. See "Create a Deployment" in *DMA Quick Start Tutorial* for instructions.
5. On the Parameters tab, specify values (or set the type to Runtime Value) for the required parameters listed in step 2 and any additional parameters that you have exposed. You do not need to specify values for those parameters whose default values are appropriate for your environment.
6. On the Targets tab, specify one or more targets for this deployment.
7. Save the deployment (click **Save** in the lower right corner).
8. Run the workflow using this deployment, specifying any runtime parameters. See "Run Your Workflow" in *(DMA Quick Start Tutorial* for instructions.

To verify the results:

The workflow will complete and report SUCCESS on the Console if it has run successfully. If an error occurs during workflow execution, the error is logged, and the workflow terminates in the FAILURE state.

Parameters for DB2 - Configure HADR Database

The following tables describe the required and optional input parameters for this workflow.

Parameters Defined in this Step: Gather DB2 Source and Destination Instances

Parameter Name	Example Value	Description
DB2 Destination HADR Instance	hadr105 [aixom02.mycompany.com]	Required: The standby node instance name of the remote server. Administration tools,

Parameters Defined in this Step: Gather DB2 Source and Destination Instances, continued

Parameter Name	Example Value	Description
		such as the DB2 Control Center, use this parameter to contact the remote server. In the bridge execution workflow, this instance will be used at the run time to run the specific steps configured to run on the standby instance node. The value will be set at the run time.
DB2 Source HADR Instance	hadr105 [aixom01.mycompany.com]	Required: The primary node instance name of the local server. Administration tools, such as the DB2 Control Center, use this parameter to contact the local server. In the bridge execution workflow, this instance will be used at the run time to run the specific steps configured to run on the primary instance node. The value will be set at the run time.

Parameters Defined in this Step: Gather Parameters for Configure DB2 HADR

Parameter Name	Example Value	Description
DB2 HADR Database Name	DB2_HADR	Required: The database name for which the High Availability Disaster Recovery will be configured. The database name must be available on the primary instance node.
DB2 HADR Local Service Name	DB2_HADR_SERVICE_P1	Required: This parameter specifies the TCP service name for which the local high availability disaster recovery (HADR) process accepts connections.
DB2 HADR Port Number	58234	Required: This parameter specifies the TCP service port number for which the high availability disaster recovery (HADR) process accepts connections. The same port will be used in the primary and standby node for HADR communication.
DB2 HADR Remote Instance Name	hadr105	Required: This parameter specifies the instance name of the remote server. Administration tools, such as the DB2 Control Center, use this parameter to contact the remote server. High availability disaster recovery (HADR) also checks whether a remote database requesting a connection belongs to the declared remote instance.
DB2 HADR Remote Service Name	DB2_HADR_SERVICE_P1	Required: This parameter specifies the TCP service name for which the remote high availability disaster recovery (HADR) process accepts connections.
DB2 HADR Standby Host Name	aixom2.mycompany.com	Required: This parameter specifies the TCP/IP host name or IP address of the remote high

Parameters Defined in this Step: Gather Parameters for Configure DB2 HADR, continued

Parameter Name	Example Value	Description
		availability disaster recovery (HADR) database server.

DB2 - Configure Tivoli SAMP on HADR Database

This workflow configures IBM DB2 High Availability Disaster Recovery (HADR) with Tivoli System Automation for Multiplatforms (TSAMP) using db2haicu utility.

This workflow configures DB2 database(s) for IBM DB2 LUW (Linux, UNIX, and Windows) on the target source and destination servers with TSAMP where this workflow is deployed. It currently supports DB2 versions 10.1 and 10.5 on Red Hat Linux and AIX servers. This is an instance level workflow. It validates DB2 installation exist on primary and standby cluster nodes. It configures the HADR database with TSAMP. This workflow supports cluster network configuration.

This workflow supports the following:

1. To generate the default primary and standby TSAMP XML configuration files and configure HADR database with TSAMP.
2. To deploy a user specified golden template of the DB2 HADR TSAMP XML configuration file on primary and to use a default standby configuration for TSAMP.
3. To deploy a user specified golden template of the DB2 HADR TSAMP XML configuration file on standby and to use a default primary configuration for TSAMP.
4. To use a user specified golden template of the primary and standby TSAMP XML configuration files and configure TSAMP on HADR Database.

To use this workflow in your environment, see the following information:

Topic	Information Included
"Prerequisites" on the next page	List of prerequisites that must be satisfied before you can run this workflow
"How this Workflow Works" on page 89	Information about what the workflow does, including validation checks performed, steps executed, and step descriptions
"How to Run this Workflow" on page 91	Instructions for running this workflow in your environment

Topic	Information Included
"Parameters for Configure Tivoli SAMP on HADR Database" on page 94	List of input parameters for this workflow

Prerequisites

Before performing the procedures in this section, your environment must meet the following minimum requirements:

- SSH service must be turned on for both primary and standby host computers.
- The source and destination host computer is configured with SSH password-less login across the nodes (primary to standby and vice versa).
- DB2 software must be provisioned on both the primary and standby host computer.

Tip: You can use DB2 - Provision Software workflow to accomplish this.

- The DB2 instance must be provisioned on both primary and standby host computer.

Tip: You can use DB2 - Provision Instance workflow to accomplish this.

- The DB2 database must be available on primary and standby instance cluster node with primary and standby HADR configuration state.
- DB2 instance on primary host computer must be up and running on both the primary and standby host computer.
- Tivoli System Automation for Multiplatforms (TSAMP) must be installed and on both primary and standby cluster nodes.
- Valid license to activate the TSAMP on primary and standby cluster nodes.
- Guidelines from IBM to provide the correct input parameter values for the steps Gather Parameters For Configure Tivoli SAMP on HADR Database and Gather Advanced Parameters For Configure Tivoli SAMP on HADR Database in order to prepare correct XML file for TSAMP.
- The following workflow requirements:

Workflow	Requirements
DB2 - Configure Tivoli SAMP on HADR Database	<p>The sudo package is installed on the target servers.</p> <p>The target servers have the gunzip and tar utilities in the environment path.</p>

Refer to the [IBM Documentation](#) for the following:

- Complete installation and infrastructure requirements for IBM DB2.
- Acceptable types and range of values when using DMA advanced parameters to configure IBM DB2 HADR settings.

How this Workflow Works

This workflow performs the following actions:

Configures IBM DB2 HADR with Tivoli System Automation for Multiplatforms (TSAMP) using db2haicu utility.

Steps Executed

The DB2 - Configure Tivoli SAMP On HADR Database workflow includes the following steps. Each step must complete successfully before the next step can start. If a step fails, the workflow reports a failure and all subsequent steps are skipped.

Steps Used by DB2 - Configure Tivoli SAMP On HADR Database

Workflow Step	Description
Gather DB2 Source and Destination Instances	This step gathers data on DB2 source and destination HADR instances.
Gather Parameters For Configure Tivoli SAMP on HADR Database	This step accepts mandatory parameters for the workflow.
Gather Advanced Parameters For Configure Tivoli SAMP on HADR Database	This step accepts optional parameters for the workflow.
Validate Parameters For Configure Tivoli SAMP On Primary Node	This step validates all the input parameter values received in the gather and advanced gather input parameter steps, validate the DB2 target and make sure it meets all the necessary criteria to setup the Tivoli SAMP on the given targets.
Validate Parameters For Configure Tivoli SAMP On Standby Node	This step validates all the input parameter values received in the gather and advanced gather input parameter steps, validate the DB2 target and make sure it meets all the necessary criteria to setup the Tivoli SAMP on the given targets.
Download Software	This step automates the transfer of files from the SA Software Library to individual managed servers for use in downstream workflow steps. Verifies checksum of each file transferred.
Setup ACR On Primary Cluster Node	This step configures the HADR database to activate for automatic client rerouting feature in the event of failover.
Setup Peer Cluster Domain On Primary Node	This step configures the hosts to activate with Reliable Scalable Cluster Technology for each node.

Steps Used by DB2 - Configure Tivoli SAMP On HADR Database , continued

Workflow Step	Description
Cleanup On Failure For Tivoli SAMP Primary Node	This step deconfigures the TSA if configured partially with some failure or in the event of any step failure. It also clears up all the temporary files that is being generated during the Tivoli SAMP setup.
Setup ACR On Standby Cluster Node	This step configures the HADR database to activate for automatic client rerouting feature in the event of failover.
Cleanup On Failure For Tivoli SAMP Standby Node	This step deconfigures the TSA if configured partially with some failure or in the event of any step failure. It also clears up all the temporary files that is being generated during the Tivoli SAMP setup.
Setup Peer Cluster Domain On Standby Node	This step configures the hosts to activate with Reliable Scalable Cluster Technology for each node.
Configure HA Instance On Standby Node	This step prepares the XML configuration file based on user input parameters and runs it using db2haicu IBM utility to configure the Tivoli SAMP with cluster domain for standby cluster node.
Verify Cluster Resources On Standby Node	This step verifies if the target instance and database is configured for HADR and set with automatic failover in the event of failure. It checks for all the possible resources and prints those out on the steplog for the user information.
Configure HA Instance On Primary Node	This step prepares the XML configuration file based on user input parameters and runs it using db2haicu IBM utility to configure the Tivoli SAMP with cluster domain for primary cluster node.
Cleanup On Failure For Tivoli SAMP Primary Node	This step deconfigures the TSA if configured partially with some failure or in the event of any step failure. It also clears up all the temporary files that is being generated during the Tivoli SAMP setup.
Verify Cluster Resources On Primary Node	This step verifies if the target instance and database is configured for HADR and set with automatic failover in the event of failure. It checks for all the possible resources and prints those out on the steplog for the user information.
Cleanup On Failure For Tivoli SAMP Standby Node	This step deconfigures the TSA if configured partially with some failure or in the event of any step failure. It also clears up all the temporary files that is being generated during the Tivoli SAMP setup.

Results Verification

- The workflow uses the IBM utility “db2pd -d <database name>” and runs it on the primary and standby nodes. It verifies the results by parsing the resultset and looks up for the specific parameter values to confirm that the HADR setup is complete and TSAMP is setup. It also runs the command “db2pd -ha” to identify the cluster resources configured for HADR.
- The workflow uses the IBM utility “issam” to find out the “online” and “offline” status of the primary or standby nodes.
- The user can manually run the “db2 takeover hadr on database <HADR Database Name>” command on the standby node machine as an instance user. This performs the failover test and

verifies that the takeover was performed and it switches the standby to primary and the primary to standby database.

- The user can run the “db2_kill” command on primary cluster node machine as an instance user and verify the status of cluster nodes after few mins to make sure failover is performed successfully.

How to Run this Workflow

The following instructions show you how to customize and run the DB2 - Configure Tivoli SAMP On HADR Database workflow in your environment.

Tip: For detailed instructions to run DMA workflows, see *HPE DMA Quick Start Tutorial*.

The workflow provides default values for some parameters. These default values are usually sufficient for a "typical" installation. You can override the defaults by specifying parameter values in the deployment. You can also expose additional parameters in the workflow, if necessary, to accomplish more advanced scenarios. Any parameters not explicitly specified in the deployment will have the default values listed in ["Parameters for Configure Tivoli SAMP on HADR Database" on page 94](#).

Note: Before following this procedure, review the ["Prerequisites" on page 88](#), and ensure that all requirements are satisfied.

To use the DB2 - Configure Tivoli SAMP On HADR Database workflow:

1. Create a deployable copy of the workflow (see "Create a Deployable Workflow" in *HPE DMA Quick Start Tutorial*)

- a. Determine the values that you will specify for the following parameters.

Parameters Defined in this Step: Gather DB2 Source and Destination Instances

Parameter Name	Example Value	Description
DB2 Destination HADR Instance	hadr105 [aixom02.mycompany.com]	The standby node instance name of the remote server. Administration tools, such as the DB2 Control Center, use this parameter to contact the remote server. In the bridge execution workflow, this instance will be used at the run time to run the specific steps configured to run on the standby instance node. The value will be set at the run time.
DB2 Source HADR Instance	hadr105 [aixom01.mycompany.com]	The primary node instance name of the local server. Administration tools, such as the DB2 Control Center, use this parameter to contact the local server. In the bridge execution workflow, this instance will be used at the run time to run the specific steps configured to run on the primary instance node. The value will be set at the run time.

Gather Parameters For Configure Tivoli SAMP on HADR Database

Parameter Name	Example Value	Description
Database Name	DB2HADR	The database name for which the High Availability Disaster Recovery will be configured. The database must be available on the primary and standby instance cluster nodes.
IP Of Primary Cluster Node	16..0.0.1	Internet Protocol Address (IP address) for primary cluster node machine where the HADR Instance and database is configured.
IP Of Standby Cluster Node	16.0.0.2	Internet Protocol Address (IP address) for primary cluster node machine where the HADR Instance and database is configured.
Local Instance Name	DB2_105HADR_SVC1	This parameter specifies the instance name of the local cluster node. Administration tools, such as the DB2 Control Center, use this parameter to contact the local server. High availability disaster recovery (HADR) also checks whether a local database requesting a connection belongs to the declared local instance. Default, it is configured to use the instance name on which this workflow is deployed.)

Gather Parameters For Configure Tivoli SAMP on HADR Database, continued

Parameter Name	Example Value	Description
Local Instance Port Number	51000	DB2 connection port number for the local instance on primary cluster node where HADR database is mounted.
Primary Cluster Node Name	aixom01.mycompany.com	This parameter specifies the local host (primary cluster node name) name for high availability disaster recovery (HADR) TCP communication.
Quorum Device Name	16.0.1.1	A network quorum is an IP address that can be pinged from both the primary and the standby nodes. In the event of a site failure, the quorum decides which node serves as the active node and which node goes offline. When you are choosing the network quorum, ensure that the IP remains active all the time. The DNS server IP is always a good choice for the network quorum.
Remote Instance Name	hadr105	This parameter specifies the instance name of the remote cluster node (server). Administration tools, such as the DB2 Control Center, use this parameter to contact the remote server. High availability disaster recovery (HADR) also checks whether a remote database requesting a connection belongs to the declared remote instance.
Remote Instance Port Number	51000	DB2 connection port number for the remote instance on standby cluster node where HADR database is mounted.
Standby Cluster Node Name	aixom02.mycompany.com	This parameter specifies the remote host (standby cluster node name) name for high availability disaster recovery (HADR) TCP communication.
Subnetmask Of Primary Cluster	255.255.240.0	Subnet Mask Address(IP address) for primary cluster node machine where the HADR Instance and database is configured.
Subnetmask Of Standby Cluster	255.255.240.0	Subnet Mask Address(IP address) for standby cluster node machine where the HADR Instance and database is configured.

2. In the workflow editor, expose any additional parameters that you need. You will specify values for those parameters when you create the deployment or at runtime.
3. Save the changes to the workflow (click **Save** in the lower right corner).
4. Create a new deployment. See "Create a Deployment" in *HPE DMA Quick Start Tutorial* for instructions.

5. On the Parameters tab, specify values (or set the type to Runtime Value) for the required parameters listed in step 2 and any additional parameters that you have exposed. You do not need to specify values for those parameters whose default values are appropriate for your environment.
6. On the Targets tab, specify one or more targets for this deployment.
7. Save the deployment (click **Save** in the lower right corner).
8. Run the workflow using this deployment, specifying any runtime parameters. See "Run Your Workflow" in *(HPE DMA Quick Start Tutorial)* for instructions.

To verify the results:

The workflow will complete and report SUCCESS on the Console if it has run successfully. If an error occurs during workflow execution, the error is logged, and the workflow terminates in the FAILURE state.

Parameters for Configure Tivoli SAMP on HADR Database

The following tables describe the required and optional input parameters for this workflow.

Parameters Defined in this Step: Gather DB2 Source and Destination Instances

Parameter Name	Example Value	Description
DB2 Destination HADR Instance	hadr105 [aixom02.mycompany.com]	Required: The standby node instance name of the remote server. Administration tools, such as the DB2 Control Center, use this parameter to contact the remote server. In the bridge execution workflow, this instance will be used at the run time to run the specific steps configured to run on the standby instance node. The value will be set at the run time.
DB2 Source HADR Instance	hadr105 [aixom01.mycompany.com]	Required: The primary node instance name of the local server. Administration tools, such as the DB2 Control Center, use this parameter to contact the local server. In the bridge execution workflow, this instance will be used at the run time to run the specific steps configured to run on the primary instance node. The value will be set at the run time.

Gather Parameters For Configure Tivoli SAMP on HADR Database

Parameter Name	Example Value	Description
Database Name	DB2HADR	Required: The database name for which the High Availability Disaster Recovery will be configured. The database must be

Gather Parameters For Configure Tivoli SAMP on HADR Database, continued

Parameter Name	Example Value	Description
		available on the primary and standby instance cluster nodes.
IP Of Primary Cluster Node	16..0.0.1	Required: Internet Protocol Address (IP address) for primary cluster node machine where the HADR Instance and database is configured.
IP Of Standby Cluster Node	16.0.0.2	Required: Internet Protocol Address (IP address) for primary cluster node machine where the HADR Instance and database is configured.
Local Instance Name	DB2_105HADR_SVC1	Required: This parameter specifies the instance name of the local cluster node. Administration tools, such as the DB2 Control Center, use this parameter to contact the local server. High availability disaster recovery (HADR) also checks whether a local database requesting a connection belongs to the declared local instance. Default, it is configured to use the instance name on which this workflow is deployed.)
Local Instance Port Number	51000	Required: DB2 connection port number for the local instance on primary cluster node where HADR database is mounted.
Primary Cluster Node Name	aixom01.mycompany.com	Required: This parameter specifies the local host (primary cluster node name) name for high availability disaster recovery (HADR) TCP communication.
Quorum Device Name	16.0.1.1	Required: A network quorum is an IP address that can be pinged from both the primary and the standby nodes. In the event of a site failure, the quorum decides which node serves as the active node and which node goes offline. When you are choosing the network quorum, ensure that the IP remains active all the time. The DNS server IP is always a good choice for the network quorum.
Remote Instance Name	hadr105	Required: This parameter specifies the instance name of the remote cluster node (server). Administration tools, such as the DB2 Control Center, use this parameter to contact the remote server. High availability disaster recovery (HADR) also checks whether a remote database requesting a connection belongs to the declared remote instance.
Remote Instance Port Number	51000	Required: DB2 connection port number for the remote instance on standby cluster

Gather Parameters For Configure Tivoli SAMP on HADR Database, continued

Parameter Name	Example Value	Description
		node where HADR database is mounted.
Standby Cluster Node Name	aixom02.mycompany.com	Required: This parameter specifies the remote host(standby cluster node name) name for high availability disaster recovery (HADR) TCP communication.
Subnetmask Of Primary Cluster	255.255.240.0	Required: Subnet Mask Address(IP address) for primary cluster node machine where the HADR Instance and database is configured.
Subnetmask Of Standby Cluster	255.255.240.0	Required: Subnet Mask Address(IP address) for standby cluster node machine where the HADR Instance and database is configured.

DB2 - Provision Software v2

This workflow installs IBM DB2 LUW (Linux, Unix, Windows) software on the target where this workflow is deployed. It currently supports the DB2 Versions 9.5, 9.7, 10.1, 10.5 on Red Hat Linux and AIX servers. It will provision the software at the location specified by required input parameters in the workflow deployment.

This workflow installs IBM DB2 Software at the specified location on the target server using silent install method. To use this workflow, you must provide the DB2 software Staging Directory either on the server or in a location where it can be downloaded by the workflow. This workflow will perform a typical installation using default values for IBM DB2 response file setup parameters. The workflow will create the response file based on specified default values.

To use this workflow in your environment, see the following information:

Topic	Information Included
"Prerequisites" on the next page	List of prerequisites that must be satisfied before you can run this workflow
"How this Workflow Works" on the next page	Information about what the workflow does, including validation checks performed, steps executed, and step descriptions
"How to Run this Workflow" on page 98	Instructions for running this workflow in your environment
Parameters for DB2 - Provision Software v2	List of input parameters for this workflow

Prerequisites

Before performing the procedures in this section, your environment must meet the following minimum requirements:

- The workflow must have the unchallenged ability to become the OS administrator user (typically root on UNIX systems).
- LIC_AGREEMENT parameter value for DB2 License is defaulted and set as ACCEPT. After installing the software binaries on your target machine, the license has to be activated for the instances you are going to create.
- The workflow must have access to the IBM DB2 installation binaries, either on a network drive, on a DVD (which must be in the DVD drive) or from SA repository to deploy the software binaries.
- The following prerequisites must be satisfied before you run this workflow:
 - The infrastructure required for provisioning should be in place.
 - The operating system platform is certified for the pertinent DB2 specific version.
 - The operating system kernel parameters and shared memory is properly configured.
- There should be adequate available disk space on the target servers.
- On Linux or AIX platforms, the sudo package must be installed on the target servers.
- The target servers must have the gunzip and tar utilities in the environment path.

Refer to the [IBM Documentation](#) for other DB2 provisioning requirements.

How this Workflow Works

This workflow performs the following actions:

Installs IBM DB2 Software at the specified location on the target server using silent install method.

Steps Executed

The DB2 - Provision Software v2 workflow includes the following steps. Each step must complete successfully before the next step can start. If a step fails, the workflow reports a failure and all subsequent steps are skipped.

Steps Used by DB2 - Provision Software v2

Workflow Step	Description
Gather Parameters V2 for	This step sets all the DB2 advanced configurable parameters for DB2 Provision Software that are used in subsequent workflow steps.

Steps Used by DB2 - Provision Software v2 , continued

Workflow Step	Description
Provision DB2 Software	
Gather Advanced Parameters for Provision DB2 Software V3	This step sets all the DB2 advanced configurable parameters for DB2 Provision Software that are used in subsequent workflow steps.
Validate Provision DB2 Software V2	This step validates the disk space requirements, OS virtual memory, kernel parameters setting and appropriate OS version the specific DB2 software is supported on.
Stage DB2 Software Archive	This step validates the input staging path and binary archive file to unpack(unzip) to install the software. Depending upon the file extensions(.tar, .gz),, it chooses the right library to unzip the software binary file.
Download Software	This step automates the transfer of files from the HPE SA Software Library to individual managed servers for use in downstream workflow steps. Verifies checksum of each file transferred.
Install DB2 Software V3	This step runs db2prereqcheck utility provided by IBM to ensure that the target meets all the pre-requisite before installing software. This step generates response file based on DB2 input binary version found and use it along with db2_setup utility to install DB2 software.
Verify Provision DB2 Software V3	This step runs verifies the installation location by checking the "db2" utility executable presents. It also verifies the installation location directory size and make sure DB2 is installed. It looks for the error file if any generated during installation to make sure installation has not been failed. It executes the 'db2val' to identify if DB2 is successfully installed on the target machine.
Clean Failed DB2 Software Install	This step cleans up the archive, staging, and installation location in case of DB2 provisioning fails.
Cleanup Downloaded Files	This step removes all downloaded files and archives.

How to Run this Workflow

The following instructions show you how to customize and run the DB2 - Provision Software v2 workflow in your environment.

Tip: For detailed instructions to run DMA workflows, see *HPE DMA Quick Start Tutorial*.

The workflow provides default values for some parameters. These default values are usually sufficient for a "typical" installation. You can override the defaults by specifying parameter values in the deployment. You can also expose additional parameters in the workflow, if necessary, to accomplish more advanced scenarios. Any parameters not explicitly specified in the deployment will have the default values listed in [Parameters for DB2 - Provision Software v2](#).

Note: Before following this procedure, review the ["Prerequisites" on page 97](#), and ensure that all requirements are satisfied.

To use the DB2 - Provision Software workflow:

1. Create a deployable copy of the workflow (see "Create a Deployable Workflow" in *HPE DMA Quick Start Tutorial*)
 - a. Determine the values that you will specify for the following parameters.

The following tables describe the required and optional input parameters for this workflow.

Parameters Defined in this Step: Gather Parameters V2 for Provision DB2 Software

Parameter Name	Example Value	Description
DB2 Installation Location	/opt/ibm/db2/V10.5	Fully-qualified path where DB2 will be installed.
DB2 Software Binaries	v10.5_aix64_server_t.tar.gz	Name of the DB2 installer archive file. Obtained from IBM. If the file is not found in Staging Directory (the default is /tmp/db2_stage), it will be downloaded from the software repository.

Parameters Defined in this Step: Gather Advanced Parameters for Provision DB2 Software V3

Parameter Name	Example Value	Description
Clean on Failure	Yes	Specifies whether to clean up on workflow failure. If set to 'Yes', the workflow will clean up the downloaded files, installation location and the staging location. Valid values are 'Yes' and 'No'. The default value is 'Yes'
Clean on Success	Yes	Specifies whether to clean up on workflow success. If set to 'Yes', the workflow will clean up the downloaded files. The default value is 'Yes'.

Parameters Defined in this Step: Gather Advanced Parameters for Provision DB2 Software V3, continued

Parameter Name	Example Value	Description
DB2 Installation Type	TYPICAL	The type of DB2 installation supported by IBM. It can be either COMPACT, TYPICAL, or CUSTOM. The default value is 'TYPICAL'. If CUSTOM is set, provide the DB2 installation response file with the custom parameter values.
DB2 Product Edition	DB2_SERVER_EDITION	The edition of the product that you want to install. For example: DB2 Workgroup Edition, DB2 Enterprise Edition, etc. The default value is set to 'DB2_SERVER_EDITION' for DB2 version 10.5. Use 'ENTERPRISE_SERVER_EDITION' for DB2 versions 9.7 and 10.1.
DB2 Product Installation Language	EN	The language(s) for installing your product. If no language option is specified, English language (EN) will be installed by default.
DB2 Product License	ACCEPT	Indicate acceptance of license agreement as specified in the file in "db2/license" directory on the installation media. Default value is 'ACCEPT'.
DB2 Software User Resource File	Defaultv97.rsp Defaultv101.rsp	User specified resource file to be used during DB2 software installation.
Install Tivoli System Automation Multiplatforms	NO	Installs IBM Tivoli System Automation for Multiplatforms (SAMP) with required components, if value is set to Yes. This parameter is supported only for DB2 versions 9.5 and 9.7. Default value is NO.
Staging Directory	/tmp/db2_stage	Fully-qualified path of the directory where the DB2 installer will be extracted from archive. Will be cleaned up at end of workflow execution. Default: If no input is provided /tmp/db2_stage will be created.

2. In the workflow editor, expose any additional parameters that you need. You will specify values for those parameters when you create the deployment or at runtime.
3. Save the changes to the workflow (click **Save** in the lower right corner).
4. Create a new deployment. See "Create a Deployment" in *HPE DMA Quick Start Tutorial* for instructions.

5. On the Parameters tab, specify values (or set the type to Runtime Value) for the required parameters listed in step 2 and any additional parameters that you have exposed. You do not need to specify values for those parameters whose default values are appropriate for your environment.
6. On the Targets tab, specify one or more targets for this deployment.
7. Save the deployment (click **Save** in the lower right corner).
8. Run the workflow using this deployment, specifying any runtime parameters. See "Run Your Workflow" in *(HPE DMA Quick Start Tutorial)* for instructions.

To verify the results:

The workflow will complete and report SUCCESS on the Console if it has run successfully. If an error occurs during workflow execution, the error is logged, and the workflow terminates in the FAILURE state.

Parameters for DB2 - Provision Instance

The following tables describe the required and optional input parameters for this workflow.

Parameters Defined in this Step: Gather Parameters V2 for DB2 Provision Instance

Parameter Name	Required	Example Value	Description
DB2 Installation Location	required	/opt/ibm/db2/V10.5 <i>Use the same value specified for the DB2 Installation Location parameter for the DB2 - Provision Software deployment.</i>	Fully-qualified path of the DB2 installation where the new instance will be created.
DMA Password	required	●●●	Password for the DMA user.
DMA URL	required	DMA.Url	URL of the DMA server.
DMA User	required	dmauser	The DMA user name.
Trust SSL Certificates	required	True	If "True", this step will trust any SSL used to connect to the DMA web service.

Parameters Defined in this Step: Gather Advanced Parameters V2 for DB2 Provision Instance

Parameter Name	Required	Example Value	Description
Autostart Instance	optional	yes	Enables or disables the autostart of an instance after each time system restarts.

Parameters Defined in this Step: Gather Advanced Parameters V2 for DB2 Provision Instance, continued

Parameter Name	Required	Example Value	Description
			YES or NO option.
DB2 Connection Port	optional	50000	DB2 connection port number for the new instance. Not required if instance type is client.
DB2 Connection Protocol	optional	?	Communication protocol for the DB2 connection. It should always be tcp/ip
DB2 Connection Service Comment	optional	?	Comment for the DB2 connection service. This will be added when the service will be added in to the /etc/services file for non client instance type
DB2 Fenced User	optional	fusr105	<p>The fenced user is used to run user defined functions (UDFs) and stored procedures outside of the address space used by the DB2 database. The default user is db2fenc1.</p> <p>If any of the fenced user fields have a value, then all fenced user fields must contain values. This value is available only for Linux.</p>
DB2 Fenced User Groups	optional	fgrp105	<p>The fenced group is used to add the DB2 Fenced User. The default group is db2fadm1.</p> <p>If any of the fenced user fields have a value, then all fenced user fields must contain values. This value is available only for Linux.</p>
DB2 Fenced User Home Directory	optional	/home/fusr105	<p>The home directory of the DB2 Fenced User. If no value is specified, the instance user home directory is used.</p> <p>If any of the fenced user fields have a value, then all fenced user fields must contain values. This value is available only for Linux.</p>
DB2 Fenced User Password	optional		The password for the DB2 Fenced User. If no value is specified, the instance user password is used.

Parameters Defined in this Step: Gather Advanced Parameters V2 for DB2 Provision Instance, continued

Parameter Name	Required	Example Value	Description
			If any of the fenced user fields have a value, then all fenced user fields must contain values.
DB2 Instance Home	optional	/home/v105user	The home directory of the DB2 instance owner. This value is available only for Linux.
DB2 Instance Owner	optional	v105user	The OS user id of the DB2 instance owner. It will be the name of the instance. It is also used to construct some default values. ¹
DB2 Instance Owner Groups	optional	v105grp	The primary group of the DB2 instance owner.
DB2 Instance Owner Password	optional		The password for the DB2 Instance Owner.
DB2 Instance Type	optional	ese	Type of the instance to be created. By default, workflow creates 'Enterprise' edition Instance. Valid values are: ese, wse, client, standalone.
Diagnostic Log Path	optional	/home/v105user/sql1lib/db2dump/	The fully-qualified path for the diagnostic log. By default, DB2 sets the log path to the default database path during database creation.
Service Name	optional	db2_v105	The TCP/IP connection service name to associate with the DB2 network connection port and be configured in the /etc/services file. ²

¹This parameter is hidden by default and must be exposed when you make a copy of the workflow.²This parameter is hidden by default and must be exposed when you make a copy of the workflow.

DB2 - Provision Instance

This workflow creates IBM DB2 LUW (Linux, Unix, Windows) instance on the target server where this workflow is deployed. It currently supports the DB2 Versions 9.5, 9.7, 10.1, 10.5 on Red Hat Linux and AIX servers. It will create the DB2 Instance at the user specified DB2 instance home from the DB2 Installation Location specified by required input parameters in the workflow deployment. This workflow support to create client, standalone, enterprise, workgroup edition type of DB2 Instance. Network port and TCP/IP service will be associated for all the instances except the client instance.

This workflow creates IBM DB2 Instance at the specified location on the target server using db2icrt utility provided by IBM along with the DB2 software installation. To use this workflow, you must provide the DB2 software Installation Location (DB2 Installation Directory) on the server where you are deploying this workflow.

To use this workflow in your environment, see the following information:

Topic	Information Included
"Prerequisites" below	List of prerequisites that must be satisfied before you can run this workflow
"How this Workflow Works" on the next page	Information about what the workflow does, including validation checks performed, steps executed, and step descriptions
"How to Run this Workflow" on page 106	Instructions for running this workflow in your environment
"Parameters for DB2 - Provision Instance" on page 109	List of input parameters for this workflow

Prerequisites

Before performing the procedures in this section, your environment must meet the following minimum requirements:

- The workflow must have the unchallenged ability to become the OS administrator user (typically root on UNIX systems).
- LIC_AGREEMENT parameter value for DB2 License is defaulted and set as ACCEPT. After creating the instances, License has to be activated for it to use.
- The user who runs the workflow with the server wrapper must have the access to update the /etc/service file to configure the TCP/IP services for the DB2 network port.

- The following prerequisites must be satisfied before you run this workflow:
 - The infrastructure required for provisioning should be in place.
 - The operating system platform is certified for the pertinent DB2 specific version.
 - The operating system kernel parameters and shared memory is properly configured.

Refer to the [IBM Documentation](#) for other DB2 requirements.

How this Workflow Works

This workflow performs the following actions:

Creates IBM DB2 instance at the specified location on the target server using db2icrt utility provided by IBM along with the DB2 software installation.

Steps Executed

The DB2 - Provision Instance workflow includes the following steps. Each step must complete successfully before the next step can start. If a step fails, the workflow reports a failure and all subsequent steps are skipped.

Steps Used by DB2 - Provision Instance

Workflow Step	Description
Gather Parameters V2 for DB2 Provision Instance	This step sets all the DB2 advanced configurable parameters for DB2 Provision Instance that are used in subsequent workflow steps.
Gather Advanced Parameters for Provision DB2 Instance	This step sets all the DB2 advanced configurable parameters for DB2 Provision Instance that are used in subsequent workflow steps.
Prepare DB2 Call Wrapper	Prepare the call wrappers(server, instance) level as needed to become the owner of the DB2 Server or Instance owner user and perform the appropriate task as necessary.
Validate Provision V2 DB2 Instance Parameters	This step validates all the input parameter values received in the gather and advanced gather input parameters step, validate the DB2 target and make sure it meets all the criteria to provision DB2 instance.
Create OS User	This step create an OS user using specified information and add to an existing user group. It also creates and user group is the specified group does not exist. This step must be run as the root user.
Check DB2 Instance Type	This step checks if DB2 instance type is CLIENT from the input parameters.
DB2 Create Instance	This step creates a DB2 instance using the db2icrt command from within the DB2 installation location on the target server.
Create OS User	This step create an OS user using specified information and add to an existing user group. It also creates and user group is the specified group does

Steps Used by DB2 - Provision Instance , continued

Workflow Step	Description
	not exist. This step must be run as the root user.
Configure V2 For DB2 Instance	This step configures the basic configuration parameters and start the DB2 Instance based on provided input parameters.
Add Service For DB2 Instance	This step adds a TCP/IP service entry for the DB2 network port to services file.
Verify V2 For Provision DB2 Instance	This step verifies if the DB2 instance is created successfully and functionally available for usage.

How to Run this Workflow

The following instructions show you how to customize and run the DB2 - Provision Instance workflow in your environment.

Tip: For detailed instructions to run DMA workflows, see *DMA Quick Start Tutorial*.

The workflow provides default values for some parameters. These default values are usually sufficient for a "typical" installation. You can override the defaults by specifying parameter values in the deployment. You can also expose additional parameters in the workflow, if necessary, to accomplish more advanced scenarios. Any parameters not explicitly specified in the deployment will have the default values listed in ["Parameters for DB2 - Provision Instance" on page 109](#).

Note: Before following this procedure, review the ["Prerequisites" on page 104](#), and ensure that all requirements are satisfied.

To use the DB2 - Provision Instance workflow:

1. Create a deployable copy of the workflow (see "Create a Deployable Workflow" in *DMA Quick Start Tutorial*)
 - a. Determine the values that you will specify for the following parameters.

The following tables describe the required and optional input parameters for this workflow.

Parameters Defined in this Step: Gather Parameters V2 for DB2 Provision Instance

Parameter Name	Example Value	Description
DB2 Installation Location	/opt/ibm/db2/V10.5 <i>Use the same value specified for the DB2</i>	Fully-qualified path of the DB2 installation where the new instance will be created.

Parameters Defined in this Step: Gather Parameters V2 for DB2 Provision Instance, continued

Parameter Name	Example Value	Description
	<i>Installation Location parameter for the DB2 - Provision Software deployment.</i>	
DMA Password	●●●	Password for the DMA user.
DMA URL	DMA.Url	URL of the DMA server.
DMA User	dmauser	The DMA user name.
Trust SSL Certificates	True	If "True", this step will trust any SSL used to connect to the DMA web service.

Parameters Defined in this Step: Gather Advanced Parameters V2 for DB2 Provision Instance

Parameter Name	Example Value	Description
Autostart Instance	yes	Enables or disables the autostart of an instance after each time system restarts. YES or NO option.
DB2 Connection Port	50000	DB2 connection port number for the new instance. Not required if instance type is client.
DB2 Connection Protocol	?	Communication protocol for the DB2 connection. It should always be tcp/ip
DB2 Connection Service Comment	?	Comment for the DB2 connection service. This will be added when the service will be added in to the /etc/services file for non client instance type
DB2 Fenced User	fusr105	<p>The fenced user is used to run user defined functions (UDFs) and stored procedures outside of the address space used by the DB2 database. The default user is db2fenc1.</p> <p>If any of the fenced user fields have a value, then all fenced user fields must contain values. This value is available only for Linux.</p>

Parameters Defined in this Step: Gather Advanced Parameters V2 for DB2 Provision Instance, continued

Parameter Name	Example Value	Description
DB2 Fenced User Groups	fgrp105	<p>The fenced group is used to add the DB2 Fenced User. The default group is db2fadm1.</p> <p>If any of the fenced user fields have a value, then all fenced user fields must contain values. This value is available only for Linux.</p>
DB2 Fenced User Home Directory	/home/fusr105	<p>The home directory of the DB2 Fenced User. If no value is specified, the instance user home directory is used.</p> <p>If any of the fenced user fields have a value, then all fenced user fields must contain values. This value is available only for Linux.</p>
DB2 Fenced User Password		<p>The password for the DB2 Fenced User. If no value is specified, the instance user password is used.</p> <p>If any of the fenced user fields have a value, then all fenced user fields must contain values.</p>
DB2 Instance Home	/home/v105user	The home directory of the DB2 instance owner. This value is available only for Linux.
DB2 Instance Owner	v105user	The OS user id of the DB2 instance owner. It will be the name of the instance. It is also used to construct some default values.
DB2 Instance Owner Groups	v105grp	The primary group of the DB2 instance owner.
DB2 Instance Owner Password		The password for the DB2 Instance Owner.
DB2 Instance Type	ese	<p>Type of the instance to be created. By default, workflow creates 'Enterprise' edition Instance.</p> <p>Valid values are: ese, wse, client, standalone.</p>
Diagnostic Log Path	/home/v105user/sql1lib/db2dump/	The fully-qualified path for the diagnostic log. By default, DB2

Parameters Defined in this Step: Gather Advanced Parameters V2 for DB2 Provision Instance, continued

Parameter Name	Example Value	Description
		sets the log path to the default database path during database creation.
Service Name	db2_v105	The TCP/IP connection service name to associate with the DB2 network connection port and be configured in the <code>/etc/services</code> file.

2. In the workflow editor, expose any additional parameters that you need. You will specify values for those parameters when you create the deployment or at runtime.
3. Save the changes to the workflow (click **Save** in the lower right corner).
4. Create a new deployment. See "Create a Deployment" in *HPE DMA Quick Start Tutorial* for instructions.
5. On the Parameters tab, specify values (or set the type to Runtime Value) for the required parameters listed in step 2 and any additional parameters that you have exposed. You do not need to specify values for those parameters whose default values are appropriate for your environment.
6. On the Targets tab, specify one or more targets for this deployment.
7. Save the deployment (click **Save** in the lower right corner).
8. Run the workflow using this deployment, specifying any runtime parameters. See "Run Your Workflow" in *HPE DMA Quick Start Tutorial* for instructions.

To verify the results:

The workflow will complete and report SUCCESS on the Console if it has run successfully. If an error occurs during workflow execution, the error is logged, and the workflow terminates in the FAILURE state.

Parameters for DB2 - Provision Instance

The following tables describe the required and optional input parameters for this workflow.

Parameters Defined in this Step: Gather Parameters V2 for DB2 Provision Instance

Parameter Name	Required	Example Value	Description
DB2 Installation Location	required	/opt/ibm/db2/V10.5 <i>Use the same value specified for the DB2 Installation Location parameter for the DB2 - Provision Software deployment.</i>	Fully-qualified path of the DB2 installation where the new instance will be created.
DMA Password	required	●●●	Password for the DMA user.
DMA URL	required	DMA.Url	URL of the DMA server.
DMA User	required	dmauser	The DMA user name.
Trust SSL Certificates	required	True	If "True", this step will trust any SSL used to connect to the DMA web service.

Parameters Defined in this Step: Gather Advanced Parameters V2 for DB2 Provision Instance

Parameter Name	Required	Example Value	Description
Autostart Instance	optional	yes	Enables or disables the autostart of an instance after each time system restarts. YES or NO option.
DB2 Connection Port	optional	50000	DB2 connection port number for the new instance. Not required if instance type is client.
DB2 Connection Protocol	optional	?	Communication protocol for the DB2 connection. It should always be tcp/ip
DB2 Connection Service Comment	optional	?	Comment for the DB2 connection service. This will be added when the service will be added in to the /etc/services file for non client instance type
DB2 Fenced User	optional	fusr105	<p>The fenced user is used to run user defined functions (UDFs) and stored procedures outside of the address space used by the DB2 database. The default user is db2fenc1.</p> <p>If any of the fenced user fields have a value, then all fenced user fields must contain values. This value is available only for Linux.</p>

Parameters Defined in this Step: Gather Advanced Parameters V2 for DB2 Provision Instance, continued

Parameter Name	Required	Example Value	Description
DB2 Fenced User Groups	optional	fgrp105	<p>The fenced group is used to add the DB2 Fenced User. The default group is db2fadm1.</p> <p>If any of the fenced user fields have a value, then all fenced user fields must contain values. This value is available only for Linux.</p>
DB2 Fenced User Home Directory	optional	/home/fusr105	<p>The home directory of the DB2 Fenced User. If no value is specified, the instance user home directory is used.</p> <p>If any of the fenced user fields have a value, then all fenced user fields must contain values. This value is available only for Linux.</p>
DB2 Fenced User Password	optional		<p>The password for the DB2 Fenced User. If no value is specified, the instance user password is used.</p> <p>If any of the fenced user fields have a value, then all fenced user fields must contain values.</p>
DB2 Instance Home	optional	/home/v105user	The home directory of the DB2 instance owner. This value is available only for Linux.
DB2 Instance Owner	optional	v105user	The OS user id of the DB2 instance owner. It will be the name of the instance. It is also used to construct some default values. ¹
DB2 Instance Owner Groups	optional	v105grp	The primary group of the DB2 instance owner.
DB2 Instance Owner Password	optional		The password for the DB2 Instance Owner.
DB2 Instance Type	optional	ese	Type of the instance to be created. By default, workflow creates 'Enterprise' edition Instance.

¹ This parameter is hidden by default and must be exposed when you make a copy of the workflow.

Parameters Defined in this Step: Gather Advanced Parameters V2 for DB2 Provision Instance, continued

Parameter Name	Required	Example Value	Description
			Valid values are: ese, wse, client, standalone.
Diagnostic Log Path	optional	/home/v105user/sql1lib/db2dump/	The fully-qualified path for the diagnostic log. By default, DB2 sets the log path to the default database path during database creation.
Service Name	optional	db2_v105	The TCP/IP connection service name to associate with the DB2 network connection port and be configured in the /etc/services file. ¹

DB2 - Provision Database

This workflow creates a IBM DB2 LUW (Linux, UNIX, and Windows) Database on the target server where this workflow is deployed. It currently supports the DB2 Versions 9.5, 9.7, 10.1, 10.5 on RedHat Linux and AIX servers. It will create the DB2 Database on the instance where it is deployed with the user specified DB2 Database name required input parameters in the workflow deployment. This workflow creates databases on standalone, enterprise, workgroup edition types of DB2 Instances. This workflow is currently creates databases using automatic storage or non-automatic storage type and tablespace (catalog tablespace, user tablespace, and database tablespace) creation along with the database managed by system.

This workflow creates an IBM DB2 Database on the instance where it is deployed. It creates the directory structure for data storage under the specified directory locations on the target server using DDL (based on the input parameter values specified by user). It also creates the database using user defined DDL scripts provided in the input file. The scripts will be executed against the DB2 instance where the workflow has been deployed.

To use this workflow in your environment, see the following information:

¹This parameter is hidden by default and must be exposed when you make a copy of the workflow.

Topic	Information Included
"Prerequisites" below	List of prerequisites that must be satisfied before you can run this workflow
"How this Workflow Works" on the next page	Information about what the workflow does, including validation checks performed, steps executed, and step descriptions
"How to Run this Workflow" on page 115	Instructions for running this workflow in your environment
"Parameters for DB2 - Provision Database" on page 121	List of input parameters for this workflow

Prerequisites

Before performing the procedures in this section, your environment must meet the following minimum requirements:

- The workflow must have the unchallenged ability to become the OS administrator user (typically root on UNIX systems).
- LIC_AGREEMENT parameter value for DB2 License is defaulted and set as ACCEPT. After creating the instances, License has to be activated for it to use.
- The user who runs the workflow with the server wrapper must have the access to update the /etc/service file to configure the TCP/IP services for the DB2 network port.
- The following prerequisites must be satisfied before you run this workflow:
 - The infrastructure required for provisioning should be in place.
 - The operating system platform is certified for the pertinent DB2 specific version.
 - The operating system kernel parameters and shared memory is properly configured.
- The DMA database metadata must be up-to-date for the DB2 Instance where the workflow is deployed.
- The workflow currently does not support any raw device for provisioning database and tablespaces.
- The workflow currently does not support tablespaces (for creating catalog, user, database) managed by Database. You cannot provide the number of pages to be allocated for the tablespace sizes.
- Refer to the [IBM Documentation](#) for the complete installation and infrastructure requirements for IBM DB2.

How this Workflow Works

This workflow performs the following actions:

Creates an IBM DB2 Database on the instance where it is deployed.

Steps Executed

The DB2 - Provision Instance workflow includes the following steps. Each step must complete successfully before the next step can start. If a step fails, the workflow reports a failure and all subsequent steps are skipped.

Steps Used by DB2 - Provision Instance

Workflow Step	Description
Gather Parameters for DB2 Provision Database	This step sets the default values for call wrapper and all the DB2 Provision Database parameters for Database Creation that are used in subsequent workflow steps.
Gather Advanced Parameters for Provision DB2 Database	This step sets all the DB2 advanced configurable parameters for DB2 Provision Database that are used in subsequent workflow steps. If these parameters value provided by user, then override the user provided values for them.
Prepare DB2 Call Wrapper	Prepare the call wrappers (server, instance) level as needed to become the owner of the DB2 Server or Instance owner user and perform the appropriate task as necessary.
Validate DB2 Provision Database Parameters	This step validates all the input parameter values received in the gather and advanced gather input parameters step, validate the DB2 target and make sure it meets all the criteria to provision DB2 database.
Construct DB2 Create Database DDL	This step constructs the logic for the DDL SQL script which will then be executed in a later step to create the database or tablespaces along with the database.
Download Software	This step automates the transfer of files from the HP SA Software Library to individual managed servers for use in downstream workflow steps. Verifies checksum of each file transferred.
Create DB2 Database	This step creates DB2 Database using the DDL SQL generated in the previous step based on input parameters specified.
Run DB2 User Defined Command Line Processor Scripts	This step runs the user specified DB2 Command Line Processor (CLP) script without any pre-validations and post verifications.
Verify DB2 Provision Database	This step verifies if the specified database has been created and displays the details about the database and tablespaces.
Cleanup Downloaded Files	This step removes all downloaded files and archives.
Discover DB2 Databases	This step audits the server's physical environment looking for DB2 databases.

Steps Used by DB2 - Provision Instance , continued

Workflow Step	Description
	<p>Note: Discovery is ONLY additive. It will not remove instances or databases currently in your environment. It is the end-user's responsibility to delete content that is no longer in use.</p> <p>In cluster situations where one node is active while other nodes are inactive, Discovery will only find instances and databases on the active node. Nothing will be added to inactive nodes.</p>

How to Run this Workflow

The following instructions show you how to customize and run the DB2 - Provision Database workflow in your environment.

Tip: For detailed instructions to run DMA workflows, see *DMA Quick Start Tutorial*.

The workflow provides default values for some parameters. These default values are usually sufficient for a "typical" installation. You can override the defaults by specifying parameter values in the deployment. You can also expose additional parameters in the workflow, if necessary, to accomplish more advanced scenarios. Any parameters not explicitly specified in the deployment will have the default values listed in ["Parameters for DB2 - Provision Database" on page 121](#).

Note: Before following this procedure, review the ["Prerequisites" on page 113](#), and ensure that all requirements are satisfied.

To use the DB2 - Provision Database workflow:

1. Create a deployable copy of the workflow (see "Create a Deployable Workflow" in *DMA Quick Start Tutorial*)
 - a. Determine the values that you will specify for the following parameters.

The following tables describe the required and optional input parameters for this workflow.

Parameters Defined in this Step: Gather Parameters for DB2 Provision Database

Parameter Name	Example Value	Description
Database Name	cloud_db	Name of the DB2 database that you want to create. The name has a maximum of 8 characters without any special characters. There is no default. This parameter is used if the database is created using user provided CLP scripts.
DB2 Installation Location	/opt/ibm/db2/V10.5	Fully-qualified path where DB2 is installed on the target machine.

Parameters Defined in this Step: Gather Parameters for DB2 Provision Database, continued

Parameter Name	Example Value	Description
DMA Password	●●●	Password for the DMA user.
DMA URL	DMA.Url	URL of the DMA server.
DMA User	dmauser	The DMA user name.
Instance Home	?	Physical path of the DB2 Instance creation directory from where all the DB2 Instance level commands can be run. The instance name can be of 8 charset size.
Trust SSL Certificates	True	If "True", this step will trust any SSL used to connect to the DMA Web Service.

Parameters Defined in this Step: Gather Advanced Parameters for DB2 Provision Database

Parameter Name	Example Value	Description
Auto Configure Key	?	String to pass to AUTOCONFIGURE option. It calculates and displays initial values for the buffer pool size, database configuration and database manager configuration parameters, with the option of applying these reported values.
Auto Configure Value	?	This parameter value is mandatory if you want to enable the "CONFIGURE" parameters for the database. This is a configuration key for the "AUTOCONFIGURE" parameter to set the memory, workload, priority types of Database Manager configuration parameters.
Automatic Storage	YES	Automatic storage should be enabled for the new database or not. (YES, NO). This will enable the database with the ability to support automatic storage management. Default value is set 'YES' for this.
Automatic Storage Paths	/home/db2inst/db206 , /home/db2inst/db208	Comma-separated list of the fully-qualified paths for the automatic storage. ¹
Catalog Tablespace Path		Specifies the definition of the table space that will hold the catalog tables, SYSCATSPACE. If not specified and automatic storage is not enabled for the database, SYSCATSPACE is

¹This parameter is hidden by default and must be exposed when you make a copy of the workflow.

Parameters Defined in this Step: Gather Advanced Parameters for DB2 Provision Database, continued

Parameter Name	Example Value	Description
		created as a System Managed Space (SMS) table space with NUMSEGS number of directories as containers, and with an extent size of DFT_EXTENTSIZE. For example: /NODE0000/SQL00001/SQLT000
Code Set	utf8	The code set to be used for data entered into this database. After you create the database, you cannot change the specified code set. ¹
Collating Sequence	system	This parameter value is to identifies the type of collating sequence to be used for the database. Once the database has been created, the collating sequence cannot be changed.
Comment String	"My Development database"	This parameter describes the database entry in the database directory. Any comment that helps to describe the database can be entered. Maximum length is 30 characters. A carriage return or a line feed character is not permitted. The comment text must be enclosed by single or double quotation marks. For example: "My test database". ¹
Database Alias	tstcloud	This parameter sets an alias for the database in the system database directory (maximum of 8 characters). If no alias is provided, the specified database name is used. ¹
Database Creation Script	?	Fully qualified path of the DB2 script to create the database. If this script is provided, database is created using this script and all the other options are ignored. The script may contain <instance.name> and/or <database.name>, which will get replaced by actual instance name and database name.
Database Path	?	Fully qualified path on which to create the database. Defaults to the instance home. DBPATH ON parameter has to be used when automatic storage is enabled to keep the database information separate from the database data.
Default Extent Size	4	Specifies the number of PAGESIZE pages that will be written to a container before skipping to the next container. The extent size value can also be specified as an integer value followed by K (for kilobytes) or M (for megabytes). The

¹This parameter is hidden by default and must be exposed when you make a copy of the workflow.

Parameters Defined in this Step: Gather Advanced Parameters for DB2 Provision Database, continued

Parameter Name	Example Value	Description
		default value is provided by the dft_extent_sz database configuration parameter, which has a valid range of 2-256 pages.
Download Location	/tmp	Fully-qualified directory path where the user specified command-line processing scripts will be downloaded to use for provisioning the database.
Extent Size	?	Specifies the number of PAGESIZE pages that will be written to a container before skipping to the next container. The extent size value can also be specified as an integer value followed by K (for kilobytes) or M (for megabytes). If specified in this way, the floor of the number of bytes divided by the page size is used to determine the value for the extent size. The database manager cycles repeatedly through the containers as data is stored. This is used for the tablespace creation along with the database creation.
Is Catalog Tablespace	Y	Specify "Y" to create "catalog tablespace" along with the database explicitly. By default, it doesn't set the value "Y" so no explicit catalog tablespace will be created besides what DB2 system creates.
Is Temporary Tablespace	Y	Specify "Y" to create "temporary tablespace" along with the database explicitly. By default, it doesn't set the value "Y" so no explicit temporary tablespace will be created besides what DB2 system creates.
Is User Tablespace	Y	Specify "Y" to create "user tablespace" along with the database explicitly. By default, it doesn't set the value "Y" so no explicit user tablespace will be created besides what DB2 system creates.
Overhead	?	The I/O controller overhead and disk seek and latency time (in number of milli-seconds). This value is used to determine the cost of I/O during query optimization. For a database that was created in Version 9 or later, the default I/O controller usage and disk seek and latency time is 7.5 milliseconds. For a database that was upgraded from a previous version of DB2 to Version 9 or later, the default is 12.67 milliseconds.
Page Size	8 K	The page size of the default buffer pool and the

Parameters Defined in this Step: Gather Advanced Parameters for DB2 Provision Database, continued

Parameter Name	Example Value	Description
		<p>initial table spaces (SYSCATSPACE, TEMPSPACE1, USERSPACE1) when the database is created. Also the default page size for all future CREATE BUFFERPOOL and CREATE TABLESPACE statements. 1</p> <p>The format is <n> or <n> K, where <n> is an integer. Valid values are: 4096, 8192, 16384, 32768, 4 K, 8 K, 16 K, or 32 K. If you use the <n> K format, there must be at least one space between the integer and K.</p> <p>The default is 4096 bytes (or 4 K).</p>
Prefetch Size	32	<p>Specifies the number of PAGESIZE pages that will be read from the table space when data prefetching is being performed. The prefetch size value can also be specified as an integer value followed by K (for kilobytes), M (for megabytes), or G (for gigabytes). If specified in this way, the floor of the number of bytes divided by the page size is used to determine the number of pages value for prefetch size. Default value is 32.</p>
Restrictive	YES	<p>Restrict access to PUBLIC or not. If the RESTRICTIVE parameter is present it causes the restrict_access database configuration parameter to be set to YES and no privileges or authorities are automatically granted to PUBLIC. If the RESTRICTIVE parameter is not present then the restrict_access database configuration parameter is set to NO and privileges are automatically granted to PUBLIC.</p>
Temporary Tablespace Path	?	<p>Specifies the definition of the initial system temporary table space, TEMPSPACE1. If not specified and automatic storage is not enabled for the database, TEMPSPACE1 is created as an SMS table space with NUMSEGS number of directories as containers and with an extent size of DFT_EXTENTSIZE. For example: /NODE0000/SQL00001/.</p> <p>This parameter value is mandatory if "Is Temporary Tablespace" = "Y"</p>
Territory	US	<p>The territory or locale identifier to be used for data entered into this database. After you create the database, you cannot change the specified territory. The combination of the code set and territory must be valid. For example:</p>

Parameters Defined in this Step: Gather Advanced Parameters for DB2 Provision Database, continued

Parameter Name	Example Value	Description
		US1
Transfer Rate	?	Time to read one page into memory (in milliseconds). Specifies the time to read one page into memory. This value is used to determine the cost of I/O during query optimization. The value of number-of-milliseconds is any numeric literal (integer, decimal, or floating point). If this value is not the same for all containers, the number should be the average for all containers that belong to the table space. For a database that was created in Version 9 or later, the default time to read one page into memory is 0.06 milliseconds. For a database that was upgraded from a previous version of DB2 to Version 9 or later, the default is 0.18 milliseconds.
User Tablespace Path	?	Specifies the definition of the initial system user tablespace, USERTABLESPACE. If not specified and automatic storage is not enabled for the database, USERTABLESPACE is created as an SMS table space with NUMSEGS number of directories as containers and with an extent size of DFT_EXTENTSIZE. (ex. /u/smith/smith/NODE0000/SQL00001/). This parameter value is mandatory if "Is UserTablespace" = "Y"

2. In the workflow editor, expose any additional parameters that you need. You will specify values for those parameters when you create the deployment or at runtime.
3. Save the changes to the workflow (click **Save** in the lower right corner).
4. Create a new deployment. See "Create a Deployment" in *HPE DMA Quick Start Tutorial* for instructions.
5. On the Parameters tab, specify values (or set the type to Runtime Value) for the required parameters listed in step 2 and any additional parameters that you have exposed. You do not need to specify values for those parameters whose default values are appropriate for your environment.
6. On the Targets tab, specify one or more targets for this deployment.
7. Save the deployment (click **Save** in the lower right corner).
8. Run the workflow using this deployment, specifying any runtime parameters. See "Run Your

Workflow" in *(HPE DMA Quick Start Tutorial* for instructions.

To verify the results:

The workflow will complete and report SUCCESS on the Console if it has run successfully. If an error occurs during workflow execution, the error is logged, and the workflow terminates in the FAILURE state.

Parameters for DB2 - Provision Database

The following tables describe the required and optional input parameters for this workflow.

Parameters Defined in this Step: Gather Parameters for DB2 Provision Database

Parameter Name	Required	Example Value	Description
Database Name		cloud_db	Name of the DB2 database that you want to create. The name has a maximum of 8 characters without any special characters. There is no default. This parameter is used if the database is created using user provided CLP scripts.
DB2 Installation Location	required	/opt/ibm/db2/V10.5	Fully-qualified path where DB2 is installed on the target machine.
DMA Password	required	●●●	Password for the DMA user.
DMA URL	required	DMA.Url	URL of the DMA server.
DMA User	required	dmauser	The DMA user name.
Instance Home		?	Physical path of the DB2 Instance creation directory from where all the DB2 Instance level commands can be run. The instance name can be of 8 charset size.
Trust SSL Certificates	optional	True	If "True", this step will trust any SSL used to connect to the DMA Web Service.

Parameters Defined in this Step: Gather Advanced Parameters for DB2 Provision Database

Parameter Name	Required	Example Value	Description
Auto	optional	?	String to pass to AUTOCONFIGURE option.

Parameters Defined in this Step: Gather Advanced Parameters for DB2 Provision Database, continued

Parameter Name	Required	Example Value	Description
Configure Key			It calculates and displays initial values for the buffer pool size, database configuration and database manager configuration parameters, with the option of applying these reported values.
Auto Configure Value	optional	?	This parameter value is mandatory if you want to enable the "CONFIGURE" parameters for the database. This is a configuration key for the "AUTOCONFIGURE" parameter to set the memory, workload, priority types of Database Manager configuration parameters.
Automatic Storage	optional	YES	Automatic storage should be enabled for the new database or not. (YES, NO). This will enable the database with the ability to support automatic storage management. Default value is set 'YES' for this.
Automatic Storage Paths	optional	/home/db2inst/db206 , /home/db2inst/db208	Comma-separated list of the fully-qualified paths for the automatic storage. ¹
Catalog Tablespace Path	optional		Specifies the definition of the table space that will hold the catalog tables, SYSCATSPACE. If not specified and automatic storage is not enabled for the database, SYSCATSPACE is created as a System Managed Space (SMS) table space with NUMSEGS number of directories as containers, and with an extent size of DFT_EXTENTSIZE. For example: /NODE0000/SQL00001/SQLT000
Code Set	optional	utf8	The code set to be used for data entered into this database. After you create the database, you cannot change the specified code set. ²
Collating Sequence	optional	system	This parameter value is to identifies the type of collating sequence to be used for the database. Once the database has been created, the collating sequence cannot be changed.
Comment String	optional	"My Development database"	This parameter describes the database entry in the database directory. Any comment that helps to describe the database can be entered. Maximum length is 30 characters. A

¹This parameter is hidden by default and must be exposed when you make a copy of the workflow.²This parameter is hidden by default and must be exposed when you make a copy of the workflow.

Parameters Defined in this Step: Gather Advanced Parameters for DB2 Provision Database, continued

Parameter Name	Required	Example Value	Description
			carriage return or a line feed character is not permitted. The comment text must be enclosed by single or double quotation marks. For example: "My test database".1
Database Alias	optional	tstcloud	This parameter sets an alias for the database in the system database directory (maximum of 8 characters). If no alias is provided, the specified database name is used.1
Database Creation Script	optional	?	Fully qualified path of the DB2 script to create the database. If this script is provided, database is created using this script and all the other options are ignored. The script may contain <instance.name> and/or <database.name>, which will get replaced by actual instance name and database name.
Database Path	optional	?	Fully qualified path on which to create the database. Defaults to the instance home. DBPATH ON parameter has to be used when automatic storage is enabled to keep the database information separate from the database data.
Default Extent Size	optional	4	Specifies the number of PAGESIZE pages that will be written to a container before skipping to the next container. The extent size value can also be specified as an integer value followed by K (for kilobytes) or M (for megabytes). The default value is provided by the dft_extent_sz database configuration parameter, which has a valid range of 2-256 pages.
Download Location	optional	/tmp	Fully-qualified directory path where the user specified command-line processing scripts will be downloaded to use for provisioning the database.
Extent Size	optional	?	Specifies the number of PAGESIZE pages that will be written to a container before skipping to the next container. The extent size value can also be specified as an integer value followed by K (for kilobytes) or M (for megabytes). If specified in this way, the floor of the number of bytes divided by the page size is used to determine the value for the extent size. The database manager cycles repeatedly through the containers as data is stored. This is used for the tablespace creation along with the database creation.
Is Catalog	optional	Y	Specify "Y" to create "catalog tablespace"

Parameters Defined in this Step: Gather Advanced Parameters for DB2 Provision Database, continued

Parameter Name	Required	Example Value	Description
Tablespace			along with the database explicitly. By default, it doesn't set the value "Y" so no explicit catalog tablespace will be created besides what DB2 system creates.
Is Temporary Tablespace	optional	Y	Specify "Y" to create "temporary tablespace" along with the database explicitly. By default, it doesn't set the value "Y" so no explicit temporary tablespace will be created besides what DB2 system creates.
Is User Tablespace	optional	Y	Specify "Y" to create "user tablespace" along with the database explicitly. By default, it doesn't set the value "Y" so no explicit user tablespace will be created besides what DB2 system creates.
Overhead	optional	?	The I/O controller overhead and disk seek and latency time (in number of milliseconds). This value is used to determine the cost of I/O during query optimization. For a database that was created in Version 9 or later, the default I/O controller usage and disk seek and latency time is 7.5 milliseconds. For a database that was upgraded from a previous version of DB2 to Version 9 or later, the default is 12.67 milliseconds.
Page Size	optional	8 K	<p>The page size of the default buffer pool and the initial table spaces (SYSCATSPACE, TEMPSPACE1, USERSPACE1) when the database is created. Also the default page size for all future CREATE BUFFERPOOL and CREATE TABLESPACE statements. 1</p> <p>The format is <n> or <n> K, where <n> is an integer. Valid values are: 4096, 8192, 16384, 32768, 4 K, 8 K, 16 K, or 32 K. If you use the <n> K format, there must be at least one space between the integer and K.</p> <p>The default is 4096 bytes (or 4 K).</p>
Prefetch Size	optional	32	Specifies the number of PAGESIZE pages that will be read from the table space when data prefetching is being performed. The prefetch size value can also be specified as an integer value followed by K (for kilobytes), M (for megabytes), or G (for gigabytes). If specified in this way, the floor of the number of bytes divided by the page size is used to determine the number of pages value for prefetch size. Default value is 32.

Parameters Defined in this Step: Gather Advanced Parameters for DB2 Provision Database, continued

Parameter Name	Required	Example Value	Description
Restrictive	optional	YES	Restrict access to PUBLIC or not. If the RESTRICTIVE parameter is present it causes the restrict_access database configuration parameter to be set to YES and no privileges or authorities are automatically granted to PUBLIC. If the RESTRICTIVE parameter is not present then the restrict_access database configuration parameter is set to NO and privileges are automatically granted to PUBLIC.
Temporary Tablespace Path	optional	?	Specifies the definition of the initial system temporary table space, TEMPSPACE1. If not specified and automatic storage is not enabled for the database, TEMPSPACE1 is created as an SMS table space with NUMSEGS number of directories as containers and with an extent size of DFT_EXTENTSIZE. For example: /NODE0000/SQL00001/. This parameter value is mandatory if "Is Temporary Tablespace" = "Y"
Territory	optional	US	The territory or locale identifier to be used for data entered into this database. After you create the database, you cannot change the specified territory. The combination of the code set and territory must be valid. For example: US1
Transfer Rate	optional	?	Time to read one page into memory (in milliseconds). Specifies the time to read one page into memory. This value is used to determine the cost of I/O during query optimization. The value of number-of-milliseconds is any numeric literal (integer, decimal, or floating point). If this value is not the same for all containers, the number should be the average for all containers that belong to the table space. For a database that was created in Version 9 or later, the default time to read one page into memory is 0.06 milliseconds. For a database that was upgraded from a previous version of DB2 to Version 9 or later, the default is 0.18 milliseconds.
User Tablespace Path	optional	?	Specifies the definition of the initial system user tablespace, USERTABLESPACE. If not specified and automatic storage is not enabled for the database, USERTABLESPACE is created as an SMS table space with NUMSEGS number of directories as containers and with an extent

Parameters Defined in this Step: Gather Advanced Parameters for DB2 Provision Database, continued

Parameter Name	Required	Example Value	Description
			size of DFT_EXTENTSIZE.(ex. /u/smith/smith/NODE0000/SQL00001/). This parameter value is mandatory if "Is UserTablespace" = "Y"

DB2 - Patch Fixpack v2

This workflow applies fixpack for IBM DB2 LUW (Linux, UNIX, and Windows) instances on the target server where this workflow is deployed. It currently supports the DB2 Versions 9.5, 9.7, 10.1, 10.5 on RedHat Linux and AIX servers. This is a server level workflow. It will apply the fixpack to the DB2 Home (also known as the DB2 Installation Directory, for example: /opt/ibm/db2/V10.5) installed on the target machine where this workflow is deployed. It updates all the instances with the fixpack of DB2 that are created against the specific DB2 Installation.

This workflow shuts down all the DB2 instances, DB2 Admin Server, and licensing daemons that are running for all the instances that are provisioned against a specific DB2 home (DB2 Installation Location). It kills all the application user connections with DB2 instances that are to be patched. It validates the eligibility for the fixpack to apply by comparing the current fixpack level on the installed DB2 against the fixpack level that user is trying to apply.

Note: This workflow applies the DB2 fix pack to the DB2 software installation directory and all instances associated with the DB2 software installation directory. (You cannot use this workflow to apply a fix pack to a subset of the instances associated with a DB2 software installation directory.)

This workflow does not update the DB2 databases with the newly applied DB2 fix pack. You will need to do that manually after you run the workflow.

The examples given are appropriate for applying a DB2 10.5 fix pack on an AIX server.

To use this workflow in your environment, see the following information:

Topic	Information Included
"Prerequisites" on the next page	List of prerequisites that must be satisfied before you can run this workflow
"How this Workflow Works" on page 128	Information about what the workflow does, including validation checks performed, steps executed, and step descriptions

Topic	Information Included
"How to Run this Workflow" on page 129	Instructions for running this workflow in your environment
"Parameters for DB2 - Patch Fixpack v2" on page 131	List of input parameters for this workflow

Prerequisites

Before performing the procedures in this section, your environment must meet the following minimum requirements:

- A server running AIX 6.1 or 7.1 or Red Hat Enterprise Linux 5 or 6. The operating system platform must be certified for the pertinent DB2 fix pack version.
- DB2 server software—version 9.5, 9.7, 10.1, or 10.5—is installed on the target and is ready to be patched.
- The infrastructure required for applying the fix pack is in place.
- All DB2 Instances are on the same initial fix pack version.
- Patch media:

The DB2 server fix pack file from IBM.

Patch installation files must be available locally or available for download from the software repository.

Note: DMA only applies DB2 server fix packs, not universal fix packs.

- Storage: A staging directory with 7-8 gigabytes available to unpack the binary file and to apply the fix pack and archive—requires about double the size of the current DB2 installation on the disk.
- The operating system kernel parameters and virtual and shared memory are properly configured to avoid any failure while applying the DB2 fix pack.
- License for DMA.
- License for DB2 Database version 9.5, 9.7, 10.1, or 10.5.

Additional requirements

For additional requirements, see the following IBM documentation:

DB2 version	IBM documentation
9.5	DB2 Version 9.5 Fix Pack
9.7	DB2 Version 9.7 Fix Pack
10.1	DB2 Version 10.1 Fix Pack
10.5	DB2 Version 10.5 Fix Pack

How this Workflow Works

This workflow performs the following actions:

Applies the fixpack for DB2 Installations.

Steps Executed

The DB2 - Patch Fixpack v2 workflow includes the following steps. Each step must complete successfully before the next step can start. If a step fails, the workflow reports a failure and all subsequent steps are skipped.

Steps Used by DB2 - Patch Fixpack v2

Workflow Step	Description
Gather Parameters to Patch Fixpack	This step accepts parameters for the workflow. All the parameters are mandatory in this step.
Gather Advanced Parameters to Patch Fixpack v2	This step accepts parameters for advanced DB2 Install Fixpack workflow step and sets defaults.
Validate Parameters for Patch Fixpack	This step validates all the input parameter values received in the gather and advanced gather input parameters steps, validates the DB2 target and makes sure it meets all the criteria to apply fixpack.
Stage Fixpack Software Archive	This step uncompresses the archive file if compressed and then extracts the files from it (tar file) under staging path.
Download Software	This step automates the transfer of files from the HPE SA Software Library to individual managed servers for use in downstream workflow steps. Verifies checksum of each file transferred.
Shutdown DB2 Instances For Patch	This step stops DB2 instances prior to applying the patch.
Apply DB2 Fixpack To DB2 Installation	This step applies DB2 fixpack to the DB2 installation location as specified by user input parameter.
Update DB2 Instances	This step updates all the instances with the newly installed fixpack executable.
Verify Patch	This step verifies if the fixpack is applied successfully as expected on the DB2

Steps Used by DB2 - Patch Fixpack v2 , continued

Workflow Step	Description
Fixpack	Installation location and all the instances have been updated well.
Restart DB2 Instances For Fixpack	This step restarts all the DB2 instances and processes provisioned against the user specified input DB2 installation location.
Discover DB2 Databases	<p>This step audits the server's physical environment looking for DB2 databases.</p> <p>Note: Discovery is ONLY additive. It will not remove instances or databases currently in your environment. It is the end-user's responsibility to delete content that is no longer in use.</p> <p>In cluster situations where one node is active while other nodes are inactive, Discovery will only find instances and databases on the active node. Nothing will be added to inactive nodes.</p>
Bind Packages To Database	This step binds various DB2 packages to databases for each instance created against current DB2 installation.
Cleanup Downloaded Files v2	This step removes all downloaded files and archives.

How to Run this Workflow

The following instructions show you how to customize and run the DB2 - Patch Fixpack v2 workflow in your environment.

Tip: For detailed instructions to run DMA workflows, see *DMA Quick Start Tutorial*.

The workflow provides default values for some parameters. These default values are usually sufficient for a "typical" installation. You can override the defaults by specifying parameter values in the deployment. You can also expose additional parameters in the workflow, if necessary, to accomplish more advanced scenarios. Any parameters not explicitly specified in the deployment will have the default values listed in ["Parameters for DB2 - Patch Fixpack v2" on page 131](#).

Note: Before following this procedure, review the ["Prerequisites" on page 127](#), and ensure that all requirements are satisfied.

To use the DB2 - Patch Fixpack v2 workflow:

1. Create a deployable copy of the workflow (see "Create a Deployable Workflow" in *DMA Quick Start Tutorial*)

Determine the values that you will specify for the following parameters.

The following tables describe the required and optional input parameters for this workflow.

Parameters Defined in this Step: Gather Parameters to Patch Fixpack

Parameter Name	Example Value	Description
DB2 Installation Location	/opt/ibm/db2/V10.5	Fully qualified path where DB2 is installed on the target server.
Fixpack Patch Archive	v10.1fp3_linuxx64_server.tar.gz	Fully qualified file name of DB2 fixpack archive. If the file is not found in Staging Directory), it will be downloaded from the software repository.

Parameters Defined in this Step: Gather Advanced Parameters to Patch Fixpack v2

Parameter Name	Example Value	Description
Download Location	/tmp/archive	Fully qualified directory path where the user specified fixpack file will be downloaded to use it for applying fixpack.
Rebind Packages To Database	Yes	Flag to enable or disable binding capability of workflow step for various packages to databases for each instance created against current DB2 installation. Default value is "false" which will not bind any packages. Valid values are "yes", "y", "true", "false", "n", and "no".
Staging Location	/tmp/staging	Fully qualified path of the directory where DB2 installer will be extracted from archive. Will be cleaned up at end of workflow execution.
Web Service Password	●●●	Password for the HPE DMA Discovery web service API.
Web Service URL		URL for the HP DMA Discovery web service API to discover and update metadata in DMA.
Web Service User	dmawebuser	User who is capable of modifying the managed environment by using the HPE DMA Discovery web service API.

- In the workflow editor, expose any additional parameters that you need. You will specify values for those parameters when you create the deployment or at runtime.
- Save the changes to the workflow (click **Save** in the lower right corner).

4. Create a new deployment. See "Create a Deployment" in *DMA Quick Start Tutorial* for instructions.
5. On the Parameters tab, specify values (or set the type to Runtime Value) for the required parameters listed in step 2 and any additional parameters that you have exposed. You do not need to specify values for those parameters whose default values are appropriate for your environment.
6. On the Targets tab, specify one or more targets for this deployment.
7. Save the deployment (click **Save** in the lower right corner).
8. Run the workflow using this deployment, specifying any runtime parameters. See "Run Your Workflow" in *DMA Quick Start Tutorial* for instructions.

To verify the results:

The workflow will complete and report SUCCESS on the Console if it has run successfully. If an error occurs during workflow execution, the error is logged, and the workflow terminates in the FAILURE state.

Parameters for DB2 - Patch Fixpack v2

The following tables describe the required and optional input parameters for this workflow.

Parameters Defined in this Step: Gather Parameters to Patch Fixpack

Parameter Name	Required	Example Value	Description
DB2 Installation Location	required	/opt/ibm/db2/V10.5	Fully qualified path where DB2 is installed on the target server.
Fixpack Patch Archive	required	v10.1fp3_linuxx64_server.tar.gz	Fully qualified file name of DB2 fixpack archive. If the file is not found in Staging Directory), it will be downloaded from the software repository.

Parameters Defined in this Step: Gather Advanced Parameters to Patch Fixpack v2

Parameter Name	Required	Example Value	Description
Download Location	optional	/tmp/archive	Fully qualified directory path where the

Parameters Defined in this Step: Gather Advanced Parameters to Patch Fixpack v2, continued

Parameter Name	Required	Example Value	Description
			user specified fixpack file will be downloaded to use it for applying fixpack.
Rebind Packages To Database	optional	Yes	Flag to enable or disable binding capability of workflow step for various packages to databases for each instance created against current DB2 installation. Default value is "false" which will not bind any packages. Valid values are "yes", "y", "true", "false", "n", and "no".
Staging Location	optional	/tmp/staging	Fully qualified path of the directory where DB2 installer will be extracted from archive. Will be cleaned up at end of workflow execution.
Web Service Password	optional	●●●	Password for the HPE DMA Discovery web service API.
Web Service URL	optional		URL for the HP DMA Discovery web service API to discover and update metadata in DMA.
Web Service User	optional	dmawebuser	User who is capable of modifying the managed environment by using the HPE DMA Discovery web service API.

DB2 - Rollback Fixpack v2

This workflow can roll back server or universal fixpack for IBM DB2 LUW (Linux, UNIX, and Windows) instances on the target server where this workflow is deployed. It currently supports the DB2 Versions 9.5, 9.7, 10.1, 10.5 on RedHat Linux and AIX servers. This is a server level workflow. It will rollback fixpack to the DB2 Home (also known as the DB2 Installation Directory, for example: /opt/ibm/db2/V10.5) installed on the target machine where this workflow is deployed. It updates all the instance(s) by restoring the backup provided by the user.

This workflow shuts down all the DB2 instances, DB2 Admin Server, and licensing daemons that are running for all the instances that are provisioned against a specific DB2 home (DB2 installation location). It kills all the application user connections with DB2 instances that are to be rolled back. It validates the eligibility for the fixpack to rollback by comparing the current fixpack level on the installed DB2 against the fixpack level that user is trying restore from the backup.

The workflow also rebinds the OS packages with databases for each instance, if exists.

To use this workflow in your environment, see the following information:

Topic	Information Included
"Prerequisites" below	List of prerequisites that must be satisfied before you can run this workflow
"How this Workflow Works" on the next page	Information about what the workflow does, including validation checks performed, steps executed, and step descriptions
"How to Run this Workflow" on page 135	Instructions for running this workflow in your environment
"Parameters for DB2 - Rollback Fixpack v2" on page 139	List of input parameters for this workflow

Prerequisites

Before performing the procedures in this section, your environment must meet the following minimum requirements:

- A server running AIX 6.1 or 7.1 or Red Hat Enterprise Linux 5 or 6. The operating system platform must be certified for the pertinent DB2 fix pack version.
- DB2 server software—version 9.5, 9.7, 10.1, or 10.5—is installed on the target and fixpack applied.
- The workflow must have the unchallenged ability to become the OS administrator user (typically root on UNIX systems).
- For all the instances on the target machine, the license has to be activated to use; otherwise the workflow will not be able to restart the instances after the fixpack is rolled back and database connection may not be possible again.
- The user who runs the workflow with the server wrapper must have the access to create or modify the directory structure for instances and databases.
- As stated in the IBM DB2 release bulletin, the following prerequisites must be satisfied before this workflow is run:
 - DB2 software must be already installed on the target machine.
 - The infrastructure required for rollback fixpack must be in place. Make sure the target server has adequate available disk space to rollback and restore DB2 installation. By default, it is expected to have about double the size of current DB2 Installation on the disk.

- The operating system platform is certified for the pertinent DB2 specific fixpack version.
- The operating system kernel parameters and virtual and shared memory is properly configured to avoid any failure while applying the DB2 fixpack.
- All DMA database metadata must be up-to-date on the target server where the workflow is deployed.

Additional requirements

For additional requirements, see the following IBM documentation:

DB2 version	IBM documentation
9.5	DB2 Version 9.5 Fix Pack
9.7	DB2 Version 9.7 Fix Pack
10.1	DB2 Version 10.1 Fix Pack
10.5	DB2 Version 10.5 Fix Pack

How this Workflow Works

This workflow performs the following actions:

Rolls back fixpack from DB2 installations.

Steps Executed

The DB2 - Patch Rollback Fixpack v2 workflow includes the following steps. Each step must complete successfully before the next step can start. If a step fails, the workflow reports a failure and all subsequent steps are skipped.

Steps Used by DB2 - Patch Fixpack v2

Workflow Step	Description
Gather Parameters for Rollback Fixpack	This step accepts parameters for the workflow DB2 Rollback Fixpack from the user. All the parameters are mandatory in this step.
Gather Advanced Parameters for Rollback Fixpack v2	This step accepts optional parameter values for DB2 Rollback Fixpack and set them up.
Validate Parameters For Rollback Fixpack v2	This step validates all the input parameter values received in the gather and advanced gather input parameters steps, validates the DB2 target and makes sure it meets all the criteria to rollback fixpack.

Steps Used by DB2 - Patch Fixpack v2 , continued

Workflow Step	Description
Stage Fixpack Software Archive v2	This step uncompresses the archive file if compressed and then extracts the files from it (tar file) under staging path.
Download Software	This step automates the transfer of files from the HPE SA Software Library to individual managed servers for use in downstream workflow steps. Verifies checksum of each file transferred.
Shutdown Instances and Admin Server	This step scans for all the running instances and active databases against the specified DB2 installation location and shuts them down.
Backup Current Installation v2	This step takes backup of the current DB2 installation before the rollback process for the fixpack.
Restore Installation From Backup v2	This step swaps the existing DB2 installation with the user provided backed up copy of DB2 installation and restores it.
Deinstall Fixpack Patch	This step rolls back fix pack from DB2 installations.
Restart DB2 Instances For Fixpack	This step restarts all the DB2 instances and processes provisioned against the user specified input DB2 installation location.
Copy Directory	This step creates a backup copy of the entire DB2 installation folder.
Update Instances To Rollback Fixpack	This step updates all the instances with the restored fixpack executables.
Restart Instances and Admin Server	This step restarts all the DB2 instances and processes provisioned against the user specified input DB2 installation location.
Verify Rollback Fixpack	This step verifies if the fixpack is rolled back successfully as expected for DB2 server.
Discover DB2 Databases	<p>This step audits the server's physical environment looking for DB2 databases.</p> <p>Note: Discovery is ONLY additive. It will not remove instances or databases currently in your environment. It is the end-user's responsibility to delete content that is no longer in use.</p> <p>In cluster situations where one node is active while other nodes are inactive, Discovery will only find instances and databases on the active node. Nothing will be added to inactive nodes.</p>
Bind Packages To Database	This step binds various DB2 packages to databases for each instance created against current DB2 installation.

How to Run this Workflow

The following instructions show you how to customize and run the DB2 - Rollback Fixpack v2 workflow in your environment.

Tip: For detailed instructions to run DMA workflows, see *DMA Quick Start Tutorial*.

The workflow provides default values for some parameters. These default values are usually sufficient for a "typical" installation. You can override the defaults by specifying parameter values in the deployment. You can also expose additional parameters in the workflow, if necessary, to accomplish more advanced scenarios. Any parameters not explicitly specified in the deployment will have the default values listed in ["Parameters for DB2 - Rollback Fixpack v2" on page 139](#).

Note: Before following this procedure, review the ["Prerequisites" on page 133](#), and ensure that all requirements are satisfied.

To use the DB2 - Rollback Fixpack v2 workflow:

1. Create a deployable copy of the workflow (see "Create a Deployable Workflow" in *DMA Quick Start Tutorial*)

Determine the values that you will specify for the following parameters.

The following tables describe the required and optional input parameters for this workflow.

Parameters Defined in this Step: Gather Parameters for Rollback Fixpack

Parameter Name	Example Value	Description
Backup Location For Installation	/opt/apps/db2/bkp/v10.5_bkp	Absolute directory path for DB2 Installation location where you want to create the backup copy of the current DB2 installation.
Backup Location to Restore	/opt/apps/db2/bkp/v10.5_bkp_to_restore	Absolute directory path for DB2 Installation location that you would like to restore for the rollback of the fixpack. Default value is False.
DB2 Installation Location	/opt/ibm/db2/v10.5	Absolute directory path for DB2 Installation location on the target machine.

Parameters Defined in this Step: Gather Advanced Parameters for Rollback Fixpack v2

Parameter Name	Example Value	Description
Clean On Success	Yes	Flag that determines whether to clean up after workflow is run successfully. The default value is 'Yes'.
Clean on Failure	Yes	Flag that determines whether to clean up after workflow failed. The default value is 'Yes'.
DB2 Fixpack Or Software Archive		This is used if the parameter "Is delInstall FixPack" is set to "Yes", "True", or "Y". For example: v10.1fp3_linuxx64_server.tar.gz
Download Location		Specifies the location to download the binary from SA.
Is Restore Fixpack From Backup		Specifies whether the rollback is accomplished

Parameters Defined in this Step: Gather Advanced Parameters for Rollback Fixpack v2, continued

Parameter Name	Example Value	Description
		by restoring the DB2 installation from a backup folder. Valid values are "Yes", "Y", "True", "False", "N", or "No".
Is deinstall Fixpack		Specifies whether the rollback is accomplished by using installFixPack tool, part of software binary. Valid values are "Yes", "Y", "True", "False", "N", or "No".
Rebind Packages To Database	False	Enables or disables binding capability of workflow step for various packages to database(s) for each instance(s) created against current DB2 installation. Valid values are "Yes", "Y", "True", "False", "N", or "No". Default value is "False" which will not bind any packages.
Staging Location	/tmp/staging	Specifies a location to stage the rollback binary. Default value is /tmp/staging.
Web Service Password		Password for the discovery web service API. If password is not provided, the DMA token is used as the password.
Web Service URL	dma.url	URL for the HPE DMA Discovery web service API to discover and update metadata in DMA. Default value is DMA.URL.
Web Service User	dma.user	User capable of modifying the managed environment through the discovery web service API.

2. In the workflow editor, expose any additional parameters that you need. You will specify values for

those parameters when you create the deployment or at runtime.

3. Save the changes to the workflow (click **Save** in the lower right corner).
4. Create a new deployment. See "Create a Deployment" in *DMA Quick Start Tutorial* for instructions.
5. On the Parameters tab, specify values (or set the type to Runtime Value) for the required parameters listed in step 2 and any additional parameters that you have exposed. You do not need to specify values for those parameters whose default values are appropriate for your environment.
6. On the Targets tab, specify one or more targets for this deployment.
7. Save the deployment (click **Save** in the lower right corner).
8. Run the workflow using this deployment, specifying any runtime parameters. See "Run Your Workflow" in *(DMA Quick Start Tutorial* for instructions.

To verify the results:

The workflow will complete and report SUCCESS on the Console if it has run successfully. If an error occurs during workflow execution, the error is logged, and the workflow terminates in the FAILURE state.

Parameters for DB2 - Rollback Fixpack v2

The following tables describe the required and optional input parameters for this workflow.

Parameters Defined in this Step: Gather Parameters for Rollback Fixpack

Parameter Name	Required	Example Value	Description
Backup Location For Installation	required	/opt/apps/db2/bkp/v10.5_bkp	Absolute directory path for DB2 Installation location where you want to create the backup copy of the current DB2 installation.
Backup Location to Restore	required	/opt/apps/db2/bkp/v10.5_bkp_to_restore	Absolute directory path for DB2 Installation location that you would like to restore for the rollback of the fixpack. Default value is False.

Parameters Defined in this Step: Gather Parameters for Rollback Fixpack, continued

Parameter Name	Required	Example Value	Description
DB2 Installation Location	required	/opt/ibm/db2/v10.5	Absolute directory path for DB2 Installation location on the target machine.

Parameters Defined in this Step: Gather Advanced Parameters for Rollback Fixpack v2

Parameter Name	Required	Example Value	Description
Clean On Success	optional	Yes	Flag that determines whether to clean up after workflow is run successfully. The default value is 'Yes'.
Clean on Failure	optional	Yes	Flag that determines whether to clean up after workflow failed. The default value is 'Yes'.
DB2 Fixpack Or Software Archive	optional		This is used if the parameter "Is deInstall FixPack" is set to "Yes", "True", or "Y". For example: v10.1fp3_linuxx64_server.tar.gz
Download Location	optional		Specifies the location to download the binary from SA.
Is Restore Fixpack From Backup	optional		Specifies whether the rollback is accomplished by restoring the DB2 installation from a backup folder. Valid values are "Yes", "Y", "True", "False", "N", or "No".

Parameters Defined in this Step: Gather Advanced Parameters for Rollback Fixpack v2, continued

Parameter Name	Required	Example Value	Description
Is deinstall Fixpack	optional		Specifies whether the rollback is accomplished by using installFixPack tool, part of software binary. Valid values are "Yes", "Y", "True", "False", "N", or "No".
Rebind Packages To Database	optional	False	Enables or disables binding capability of workflow step for various packages to database(s) for each instance(s) created against current DB2 installation. Valid values are "Yes", "Y", "True", "False", "N", or "No". Default value is "False" which will not bind any packages.
Staging Location	optional	/tmp/staging	Specifies a location to stage the rollback binary. Default value is /tmp/staging.
Web Service Password	optional		Password for the discovery web service API. If password is not provided, the DMA token is used as the password.
Web Service URL	optional	dma.url	URL for the HPE DMA Discovery web service API to discover and update metadata

Parameters Defined in this Step: Gather Advanced Parameters for Rollback Fixpack v2, continued

Parameter Name	Required	Example Value	Description
			in DMA. Default value is DMA.URL.
Web Service User	optional	dma.user	User capable of modifying the managed environment through the discovery web service API.

DB2 - Offline HADR Fixpack Parent Flow v3

This section describes how to use DMA to create a repeatable, standardized method to quickly and accurately apply IBM DB2 fixpack for DB2 installations across an enterprise to keep fix packs current.

This workflow is a wrapper or parent workflow which launches subflows to validate and apply fixpacks on a DB2 Installation. A deployment of this workflow has to be created and appropriate values have to be provided. These deployment values will be automatically passed on to the subflows that this workflow triggers.

To use this workflow in your environment, see the following information:

Topic	Information Included
"Prerequisites" on the next page	List of prerequisites that must be satisfied before you can run this workflow
"How this Workflow Works" on page 144	Information about what the workflow does, including validation checks performed, steps executed, and a high-level process flow
"How to Run this Workflow" on page 146	Instructions for running this workflow in your environment
"Parameters for DB2 - Offline HADR Fixpack Parent Flow" on page 149	List of input parameters for this workflow

Prerequisites

Before performing the procedures in this section, your environment must meet the following minimum requirements:

- The source and destination servers must be configured with SSH password-less login across all the nodes.
- A server running AIX 6.1 or 7.1 or Red Hat Enterprise Linux 5 or 6. The operating system platform must be certified for the pertinent DB2 fix pack version.
- DB2 server software—version 9.5, 9.7, 10.1, or 10.5—is installed on the target and is ready to be patched.
- The infrastructure required for applying the fix pack is in place.
- All DB2 Instances are on the same initial fix pack version.
- Patch media:

The DB2 server fix pack file from IBM.

Patch installation files must be available locally or available for download from the software repository.

- Storage: A staging directory with 7-8 gigabytes available to unpack the binary file and to apply the fix pack and archive—requires about double the size of the current DB2 installation on the disk. By default, it is expected to have about double the size of current DB2 Installation on the disk.
- The operating system platform is certified for the pertinent DB2 specific fixpack version.
- The operating system kernel parameters and virtual and shared memory are properly configured to avoid any failure while applying the DB2 fix pack.
- License for DMA.
- License for DB2 Database version 9.5, 9.7, 10.1, or 10.5.
- The workflow must have the unchallenged ability to become the OS administrator user (typically root on UNIX systems).
- For all the instances on the target server, the license has to be activated to use; otherwise the workflow will not be able to restart the instances after the fixpack is applied and database connection may not be possible again.
- The user who runs the workflow with the server wrapper must have the access to create or modify the directory structure for instances and databases.

- All the DMA database metadata must be up-to-date on the target server where the workflow is deployed.
- For clusters, currently only IBM Tivoli is supported.

Additional requirements

For additional requirements, see the following IBM documentation:

DB2 version	IBM documentation
9.5	DB2 Version 9.5 Fix Pack
9.7	DB2 Version 9.7 Fix Pack
10.1	DB2 Version 10.1 Fix Pack
10.5	DB2 Version 10.5 Fix Pack

How this Workflow Works

The following information describes how DB2 - Offline HADR Fixpack Parent Flow v3 workflow works:

Overview

This workflow does the following things in the order shown:

- First, the workflow prepares to apply the patch. It prepares the server, determines the DB2 home, prepares the DB2 instance, and validates the input parameters. If the fixpack files do not already exist they are downloaded from SA. It determines all the pertinent fixpack information.
- Fetches the standby server details for a given primary server in the HADR environment.
- The cluster automation software disabled.
- Launches the "[DB2 - Offline HADR Apply Fixpack](#)" on page 150 workflow to apply provided fixpack on both the primary and standby servers.
- Lanuches the "[DB2 - Rollback Helper](#)" on page 172 workflow if patching fixpack on any of the servers fails. For example, if patching fixpack on standby server fails, the DB2 - Rollback Helper workflow rolls back the fixpack patch applied on primary server so that both primary and standby servers are at the same fixpack level.
- The cluster automation software is enabled.

Validation Checks Performed

Much of the validation centers on the input parameters:

- The input parameters have the proper syntax (no special characters or spaces).
- Files exist or have valid specifications.
- The supplied fixpack update applies to the current version.

Workflow Steps

Steps Used in DB2 - Offline HADR Fixpack Parent Flow v3

Workflow Step	Description
Gather Parameters Patch Fixpack Offline HADR In Parent	This step accepts parameters for the workflow.
Fetch Standbys from Primary For Offline HADR In Parent	This step fetches the standby server information in the HADR environment for a given primary server. Currently, only one standby server is supported for a primary server.
Disable Automation and HADR	This step disables the cluster automation and brings the peer domain offline.
Apply DB2 Fixpack To Offline HADR DB2 Installation	This step launches the "DB2 - Offline HADR Apply Fixpack" on page 150 workflow to apply provided fixpack on both the primary and standby servers.
Enable Automation and HADR	This step enables the cluster automation and brings the peer domain online.

For parameter descriptions and defaults, see ["Parameters for DB2 - Offline HADR Fixpack Parent Flow" on page 149](#).

How to Run this Workflow

The following instructions show you how to customize and run the DB2 - Offline HADR Fixpack Parent Flow workflow in your environment.

The workflow provides default values for some parameters. These default values are usually sufficient for a "typical" installation. You can override the defaults by specifying parameter values in the deployment. You can also expose additional parameters in the workflow, if necessary, to accomplish more advanced scenarios. Any parameters not explicitly specified in the deployment will have the default values listed in ["Parameters for DB2 - Offline HADR Fixpack Parent Flow" on page 149](#).

Note: Before following this procedure, review the ["Prerequisites" on page 143](#), and ensure that all requirements are satisfied.

To use the DB2 - Offline HADR Fixpack Parent Flow workflow:

1. Create a deployable copy of the workflow.
2. Determine the values that you will specify for the following parameters:

Input parameters in the step: Gather Parameters Patch Fixpack Offline HADR In Parent

Parameter Name	Default Value	Required	Description
Current Fixpack Archive	no default	required	Fully qualified file name of DB2 fixpack archive which is currently applied to the DB2 Installation.
DB2 HADR Database Name	no default	required	The name of the DB2 database configured for HADR. For multiple instance patching, the parameter should be blank.
DB2 HADR Instance Name	no default	required	The name of the DB2 instance configured for HADR. For multiple instance patching, the parameter should be blank.
DB2 Installation Location	no default	required	Fully qualified path where DB2 is installed on the target server.
Download Location	/tmp	required	Fully qualified directory path where you want to download the fixpack binary file for applying the fixpack.
Offline Backup Location	no default	optional	Fully qualified path where the offline database backup will be stored on the target server. Please note that the path should have requisite permissions so it can be accessible from all DB2 instances.

Input parameters in the step: Gather Parameters Patch Fixpack Offline HADR In Parent, continued

Parameter Name	Default Value	Required	Description
Primary Server	no default	required	The primary server hostname or IP address in the HADR pair.
Rebind Packages To Database	no default	optional	Flag to enable or disable binding capability.
Required Fixpack Archive	no default	required	Fully qualified file name of DB2 fixpack archive which is intended to be applied to the DB2 installation.
Staging Directory	/tmp/staging	required	Fully qualified path of the directory where DB2 installer will be extracted from archive. Will be cleaned up at end of workflow execution.
DB2 New Patch Installation Location	no default	optional	New DB2 patch home location.
Clean On Success	/tmp	optional	Flag that determines whether to clean up on workflow success. when set to yes , the workflow will clean up the downloaded files. The default value is False .
Clean On Failure	/tmp	optional	Flag that determines whether to clean up on workflow failure. If set to yes , the workflow will clean up the downloaded files. The default value is False .
Standby Servers	no default	optional	FQDN of DB2 standby server name, separated by space, Name of DB2 standby server as in DB2 configuration.

Note: See ["Parameters for DB2 - Offline HADR Fixpack Parent Flow"](#) on page 149 for detailed descriptions of all input parameters for this workflow, including default values.

3. In the workflow editor, expose any additional parameters that you need . You will specify values for those parameters when you create the deployment.
4. Save the changes to the workflow (click **Save** in the lower right corner).
5. Create a new deployment.
6. On the Parameters tab, specify values for the required parameters listed in step 2 and any additional parameters that you have exposed. You do not need to specify values for those parameters whose default values are appropriate for your environment.
7. On the Targets tab, specify one or more targets for this deployment.

Note: The target for this workflow is an instance.

8. Save the deployment (click **Save** in the lower right corner).
9. Run the workflow using this deployment.

To verify the results:

The workflow will complete and report SUCCESS on the Console if it has run successfully. If an error occurs during workflow execution, the error is logged, and the workflow terminates in the FAILURE state.

Parameters for DB2 - Offline HADR Fixpack Parent Flow

The following tables describe the required and optional input parameters for this workflow. Several of these parameters are not initially visible in a deployment. For many parameters, if you do not specify a value for a parameter, a default value is assigned.

Parameters in the step: Gather Parameters Patch Fixpack Offline HADR In Parent

Parameter Name	Default Value	Required	Example Value	Description
Current Fixpack Archive	no default	required	/opt/ibm/db2/V10.5	Fully qualified file name of DB2 fixpack archive which is currently applied to the DB2 Installation. (Example v10.1fp2_linuxx64_server.tar.gz)
DB2 HADR Database Name	no default	required		The name of the DB2 database configured for HADR. For multiple instance patching, the parameter value should be blank.
DB2 HADR Instance Name	no default	required		The name of the DB2 instance configured for HADR. For multiple instance patching, the parameter value should be blank.
DB2 Installation Location	no default	required	opt/ibm/db2/V10.5	Fully qualified path where DB2 is installed on the target server.
Download Location	/tmp	required	/tmp/archive	Fully qualified directory path where the user specified fixpack file will be downloaded to use it for applying fixpack.
Offline Backup Location	no default	required	/tmp/backup	Fully qualified path where the offline database backup will be stored on the target server. Please note that the path should have requisite permissions so it can be accessible from all DB2 instances.
Primary Server	no default	required		The primary server hostname or IP address in the HADR pair.
Rebind Packages To Database	no default	optional	false	Flag to enable or diable binding capability.
Required Fixpack Archive	no default	required	v10.1fp3_linuxx64_server.tar.gz	Fully qualified file name of DB2 fixpack archive which is intended to be applied to the

Parameters in the step: Gather Parameters Patch Fixpack Offline HADR In Parent, continued

Parameter Name	Default Value	Required	Example Value	Description
				DB2 installation.
Staging Directory	/tmp/staging	required	/tmp/staging	Fully qualified path of the directory where DB2 installer will be extracted from archive. Will be cleaned up at end of workflow execution.
DB2 New Patch Installation Location	no default	optional		New DB2 patch home location.
Clean On Success	/tmp	optional	false	Flag that determines whether to clean up on workflow success. If set to yes , the workflow will clean up the downloaded files. The default value is False .
Clean On Failure	/tmp	optional	false	Flag that determines whether to clean up on workflow failure. If set to yes , the workflow will clean up the downloaded files. The default value is False .
Standby Servers	no default	optional		FQDN of DB2 standby server name, separated by space, Name of DB2 standby server as in DB2 configuration.s

DB2 - Offline HADR Apply Fixpack

This section describes how to use DMA to create a repeatable, standardized method to quickly and accurately apply IBM DB2 fixpack for Offline DB2 HADR installations across an enterprise to keep fix packs current.

This workflow applies fixpack for IBM DB2 Linux, UNIX, and Windows (LUW) instances on the target server where this workflow is deployed. It currently supports the DB2 versions 9.5, 9.7, 10.1, and 10.5 on RedHat Linux and AIX servers. This is a server level workflow. It applies the fixpack to the DB2 home (also known as the DB2 installation directory) installed on the target machine where this workflow is deployed. The workflow currently applies the fixpack to all the instances against the specific DB2 Installation.

If the required Fixpack Patch Archive version is higher than the current fixpack version, then this workflow applies the patch.

If the required Fixpack Patch Archive version is lower than the current fixpack version, then this workflow rolls back the patch.

To use this workflow in your environment, see the following information:

Topic	Information Included
"Prerequisites" below	List of prerequisites that must be satisfied before you can run this workflow
"How this Workflow Works" on page 153	Information about what the workflow does, including validation checks performed, steps executed, and a high-level process flow
"How to Run this Workflow"	Instructions for running this workflow in your environment
"Parameters for DB2 - Offline HADR Apply Fixpack" on page 159	List of input parameters for this workflow

Prerequisites

Before performing the procedures in this section, your environment must meet the following minimum requirements:

- A server running AIX 6.1 or 7.1 or Red Hat Enterprise Linux 5 or 6. The operating system platform must be certified for the pertinent DB2 fix pack version.
- DB2 server software—version 9.5, 9.7, 10.1, or 10.5—is installed on the target and is ready to be patched.
- The infrastructure required for applying the fix pack is in place.
- All DB2 Instances are on the same initial fix pack version.
- Patch media:

The DB2 server fix pack file from IBM.

Patch installation files must be available locally or available for download from the software repository.

- Storage: A staging directory with 7-8 gigabytes available to unpack the binary file and to apply the fix pack and archive—requires about double the size of the current DB2 installation on the disk. By default, it is expected to have about double the size of current DB2 Installation on the disk.
- The operating system platform is certified for the pertinent DB2 specific fixpack version.

- The operating system kernel parameters and virtual and shared memory are properly configured to avoid any failure while applying the DB2 fix pack.
- License for DMA.
- License for DB2 Database version 9.5, 9.7, 10.1, or 10.5.
- The workflow must have the unchallenged ability to become the OS administrator user (typically root on UNIX systems).
- For all the instances on the target server, the license has to be activated to use; otherwise the workflow will not be able to restart the instances after the fixpack is applied and database connection may not be possible again.
- The user who runs the workflow with the server wrapper must have the access to create or modify the directory structure for instances and databases.
- All the DMA database metadata must be up-to-date on the target server where the workflow is deployed.
- If an instance update fails, you must manually bind the packages (for each database) using the command **DB2DIR/instance/db2iupdt** *instance name*.
- If DB2 admin server is installed and the update fails during fixpack, you must manually update the DB2 admin server by using the following commands:
 - **DB2DIR/instance/dasupdt** and start up the DB2 administrator server by using **su - instance name** and **db2admin start** commands
- If the database uses federation, perform the following additional binds:
 - **db2 BIND INSTHOME\sqllib\bnd\db2dsproc.bnd** blocking all grant public
 - **db2 BIND INSTHOME\sqllib\bnd\db2stats.bnd** blocking all grant public

Additional requirements

For additional requirements, see the following IBM documentation:

DB2 version	IBM documentation
9.5	DB2 Version 9.5 Fix Pack
9.7	DB2 Version 9.7 Fix Pack
10.1	DB2 Version 10.1 Fix Pack
10.5	DB2 Version 10.5 Fix Pack

How this Workflow Works

The following information describes how the DB2 - Offline HADR Apply Fixpack workflow works:

Overview

This workflow does the following things in the order shown:

- First, the workflow prepares to apply the patch. It prepares the server, determines the DB2 home, prepares the DB2 instance, and validates the input parameters. If the fixpack files do not already exist they are downloaded from SA. It determines all the pertinent fixpack information.
- Offline HADR software archives are staged, database configuration is backed up, and DB2 instances are shutdown.
- Fixpack is applied for offline HADR installation, DB2 instances, and system catalog for each database are updated.
- The workflow verifies the fixpack.
- The DB2 instances are restarted and packages are bound to the databases.
- The DB2 databases are discovered.
- Finally, the workflow cleans up files that are no longer needed.

Validation Checks Performed

Much of the validation centers on the input parameters:

- The input parameters have the proper syntax (no special characters or spaces).
- Files exist or have valid specifications.
- The supplied fixpack update applies to the current version.

Workflow Steps

Steps Used in DB2 - Offline HADR Apply Fixpack

Workflow Step	Description
Gather Parameters to Patch Offline HADR Fixpack	This step accepts parameters for the workflow. All the parameters are mandatory in this step.
Gather Advanced Parameters to Patch Offline HADR Fixpack	This step sets all the DB2 advanced configurable parameters that are used in subsequent workflow steps.
Validate Parameters for Patch Offline HADR Fixpack	This step validates all the input parameter values received, validates the DB2 target, and ensures it meets all the criteria to apply fixpack.
Stage Offline HADR Fixpack Software Archive	This step validates the input staging path and binary archive files to unpack (unzip or extract) to install the software. Depending upon the file extensions(.tar, .gz), it chooses the right library to unpack the software binary file. It also validates the disk space availability before it unpacks the binary file.
Download Software	This step automates the transfer of files from the HPE SA software library to individual managed servers for use in downstream workflow steps. Verifies checksum of each file transferred.
Capture Configuration and take full Offline Backup	This step capture various configuration details of DB2 database on the target. It also takes the offline database backup of the database.
Shutdown DB2 Instances For Offline HADR Patch	This step shuts down the DB2 processes like DAS, fault monitor, and licensing daemon before applying the fixpack.
Apply DB2 Fixpack To Offline HADR Installation	<p>This step runs the installFixpack utility from DB2 and apply the fixpack for the existing DB2 installation. This will not be installing the DB2 software but just apply the patch. If the required Fixpack Patch Archive version is higher than the current fixpack version, then this workflow applies the patch. If the required Fixpack Patch Archive version is lower than the current fixpack version, then this workflow rolls back the patch.</p> <p>As part of installFixpack run, it also updates all the instances against the DB2 installation which is patched. It does not update any database on the fixpack level that we applied. That has to be performed manually for all the databases that are created under the instances that have been patched.</p>
Update DB2 Instances For Offline HADR	This step scans the target server and discovers all the instances eligible to update with the newly installed fixpack. It will then update each instance(s) with the new fixpack installation pointing to it.
Restore to Original State	<p>This step restores the installation to its previous state. The restore is at 3 stages:</p> <ol style="list-style-type: none"> 1. Installation 2. Instance 3. Database using restore from backup

Steps Used in DB2 - Offline HADR Apply Fixpack , continued

Workflow Step	Description
	This step runs the installFixPack command at the location where Current Fixpack Archive is unpacked to revert the fixpack to its original state.
Verify Offline HADR Patch Fixpack	This step runs the db2level utility from DB2 and to verify if the existing DB2 installation is on the same fixpack level that is applied in this workflow. It also verifies if all the instances provided against the DB2 installation location are also on the same patch level as expected.
Discover DB2 Databases	<p>This step audits the server's physical environment looking for DB2 databases.</p> <p>Discovery is only additive. It will not remove instances or databases currently in your environment. It is the end-user's responsibility to delete content that is no longer in use.</p> <p>In cluster situations where one node is active while other nodes are inactive, Discovery will only find instances and databases on the active node. Nothing will be added to inactive nodes.</p>
Restart DB2 Instances For Fixpack	This step restarts all the DB2 instances and processes provisioned against the user specified input DB2 installation location.
Cleanup Downloaded Files	This step removes files and archives that were downloaded to the target system during previous workflow steps.
Bind Packages To Database	This step binds various packages to database(s) for each instance(s) created against current DB2 installation. The default value is set to "false" which will not bind any packages. If it is set to "true", binding will occur for all the database eligible for new package bindings post applying the fixpack. By doing this, databases can use the features of newly applied fixpack.

For parameter descriptions and defaults, see ["Parameters for DB2 - Offline HADR Apply Fixpack"](#) on [page 159](#).

How to Run this Workflow

The following instructions show you how to customize and run the DB2 - Offline HADR Apply Fixpack workflow in your environment.

The workflow provides default values for some parameters. These default values are usually sufficient for a "typical" installation. You can override the defaults by specifying parameter values in the deployment. You can also expose additional parameters in the workflow, if necessary, to accomplish more advanced scenarios. Any parameters not explicitly specified in the deployment will have the default values listed in ["Parameters for DB2 - Offline HADR Apply Fixpack" on page 159](#).

Note: Before following this procedure, review the ["Prerequisites" on page 151](#), and ensure that all requirements are satisfied.

To use the the DB2 - Offline HADR Apply Fixpack workflow:

1. Create a deployable copy of the workflow.
2. Determine the values that you will specify for the following parameters:

Input parameters in the step: Gather Parameters to Patch Offline HADR Fixpack

Parameter Name	Default Value	Required	Description
Current Fixpack Archive	no default	required	Fully qualified file name of DB2 fixpack archive which is currently applied to the DB2 Installation.
DB2 Installation Location	no default	required	Fully qualified path where DB2 is installed on the target server.
Required Fixpack Archive	no default	required	Fully qualified file name of DB2 fixpack archive which is intended to be applied to the DB2 Installation.

Input parameters in the step: Gather Advanced Parameters to Patch Offline HADR Fixpack

Parameter Name	Default Value	Required	Description
Clean on Success	False	optional	Determines whether to remove downloaded and extracted files as well as cleans up installed directory on successful execution of workflow. Default is set to False.
DB2 Installation Location	no default	required	Fully qualified path where DB2 is installed on the target server.
Download Location	/tmp/archive	optional	Fully qualified directory path

Input parameters in the step: Gather Advanced Parameters to Patch Offline HADR Fixpack, continued

Parameter Name	Default Value	Required	Description
			where the user specified fixpack file will be downloaded to use it for applying fixpack.
Fixpack Install Folder	no default	optional	The folder where the fixpack will be installed. If left blank, it will be installed on the DB2 installation.
Offline Backup Location	no default	optional	Fully qualified path where the offline database backup will be stored on the target server. Please note that the path should have requisite permissions so it can be accessible from all DB2 instances.
Rebind Packages To Database	False	optional	Flag to enable or disable binding capability of workflow step for various packages to database(s) for each instance(s) created against current DB2 installation. The default value is set to "false" which will not bind any packages. Valid values are "yes", "y", "true", "false", "n", or "no".
Staging Directory	/tmp/staging	optional	Fully qualified path of the directory where DB2 installer will be extracted from archive. Will be cleaned up at end of workflow execution. Default value is /tmp/staging.
Instance SSL Port	no default	optional	Comma separated list of values corresponding to an instance name. This will be used to initialize the listener port in the SSL configuration file. For example, if Instance Name Parameter value is http_instance1,http_instance2, the port values can be 1234,4321 where 1234 belongs to http_instance1 and 4321 belongs to http_instance2.
Web Service Password	no default	optional	Password for the DMA Discovery web service API to discover and update the metadata in DMA.
Web Service URL	no default	optional	URL for the DMA Discovery web service API to discover and

Input parameters in the step: Gather Advanced Parameters to Patch Offline HADR Fix-pack, continued

Parameter Name	Default Value	Required	Description
			update metadata in DMA.
Web Service User	no default	optional	User for the DMA Discovery web service API to discover and update metadata in DMA.

Note: See ["Parameters for DB2 - Offline HADR Apply Fixpack" on the next page](#) for detailed descriptions of all input parameters for this workflow, including default values.

3. In the workflow editor, expose any additional parameters that you need . You will specify values for those parameters when you create the deployment.
4. Save the changes to the workflow (click **Save** in the lower right corner).
5. Create a new deployment.
6. On the Parameters tab, specify values for the required parameters listed in step 2 and any additional parameters that you have exposed. You do not need to specify values for those parameters whose default values are appropriate for your environment.
7. On the Targets tab, specify one or more targets for this deployment.

Note: The target for this workflow is an instance.

8. Save the deployment (click **Save** in the lower right corner).
9. Run the workflow using this deployment.

To verify the results:

The workflow will complete and report SUCCESS on the Console if it has run successfully. If an error occurs during workflow execution, the error is logged, and the workflow terminates in the FAILURE state.

Parameters for DB2 - Offline HADR Apply Fixpack

The following tables describe the required and optional input parameters for this workflow. Several of these parameters are not initially visible in a deployment. For many parameters, if you do not specify a value for a parameter, a default value is assigned.

Parameters in the step: Gather Parameters to Patch Offline HADR Fixpack

Parameter Name	Default Value	Required	Example Value	Description
Current Fixpack Archive	no default	required	v10.1fp2_linuxx64_server.tar.gz	Fully qualified file name of DB2 fixpack archive which is currently applied to the DB2 Installation.
DB2 Installation Location	no default	required	/opt/ibm/db2/V10.5	Fully qualified path where DB2 is installed on the target server.
Required Fixpack Archive	no default	required	v10.1fp3_linuxx64_server.tar.gz	<p>Fully qualified file name of DB2 fixpack archive which is intended to be applied to the DB2 Installation.</p> <p>If the required Fixpack Patch Archive version is higher than the current fixpack version, then this workflow applies the patch.</p> <p>If the required Fixpack Patch Archive version is lower than the current fixpack version, then this workflow rolls back the patch.</p>

Parameters in the step: Gather Advanced Parameters to Patch Offline HADR Fixpack

Parameter Name	Default Value	Required	Example Value	Description
Clean on Success	True	optional	False	Determines whether to remove downloaded and extracted files as well as cleans up installed directory on successful execution of workflow. Default is set to False.
DB2 Installation Location	no default	required	/opt/ibm/db2/V10.5	Fully qualified path where DB2 is installed on the target server.
Download Location	/tmp/archive	optional	/tmp/archive	Fully qualified directory path where the user specified fixpack file will be downloaded to use it for applying fixpack.
Fixpack Install	no default	optional	/opt/ibm/db2/V10.5/fp2	The folder where the

Parameters in the step: Gather Advanced Parameters to Patch Offline HADR Fixpack, continued

Parameter Name	Default Value	Required	Example Value	Description
Folder				fixpack will be installed. If left blank, it will be installed on the DB2 installation.
Offline Backup Location	no default	optional	/tmp/backup	Fully qualified path where the offline database backup will be stored on the target server. Please note that the path should have requisite permissions so it can be accessible from all DB2 instances.
Rebind Packages To Database	False	optional	False	Flag to enable or disable binding capability of workflow step for various packages to database(s) for each instance(s) created against current DB2 installation. The default value is set to "false" which will not bind any packages. Valid values are "yes", "y", "true", "false", "n", or "no".
Staging Directory	/tmp/staging	optional	/tmp/staging	Fully qualified path of the directory where DB2 installer will be extracted from archive. Will be cleaned up at end of workflow execution. Default value is /tmp/staging.
Instance SSL Port	no default	optional		Comma separated list of values corresponding to an instance name. This will be used to initialize the listener port in the SSL configuration file. For example, if Instance Name Parameter value is http_instance1,http_instance2, the port values can be 1234,4321 where 1234 belongs to http_instance1 and 4321 belongs to http_instance2.
Web Service Password	no default	optional		Password for the DMA Discovery web service API to discover and update the metadata in DMA.
Web Service URL	no default	optional		URL for the DMA Discovery web service API

Parameters in the step: Gather Advanced Parameters to Patch Offline HADR Fixpack, continued

Parameter Name	Default Value	Required	Example Value	Description
				to discover and update metadata in DMA.
Web Service User	no default	optional		User for the DMA Discovery web service API to discover and update metadata in DMA.

DB2 - Offline HADR Rollback Fixpack

This section describes how to use DMA to create a repeatable, standardized method to quickly and accurately roll back IBM DB2 fixpack from a standalone Enterprise Server Edition DB2.

This workflow rolls back fixpack for IBM DB2 LUW (Linux, UNIX, and Windows) instances on the target server where this workflow is deployed. It currently supports the DB2 versions 9.5, 9.7, 10.1, 10.5 on RedHat Linux and AIX servers. This is a server level workflow. It will rollback the fixpack to the DB2 home (also known as the DB2 installation directory, for example: /opt/ibm/db2/V10.5) installed on the target machine where this workflow is deployed. It updates all the instances with the fixpack of DB2 that are created against the specific DB2 Installation.

This workflow shuts down all the DB2 instances, DB2 admin server, and licensing daemons that are running for all the instances that are provisioned against a specific DB2 home (DB2 installation location). It kills all the application user connections with DB2 instances that are to be patched. It validates the eligibility for the fixpack to apply by comparing the current fixpack level on the installed DB2 against the fixpack level that user is trying to apply.

To use this workflow in your environment, see the following information:

Topic	Information Included
"Prerequisites" on the next page	List of prerequisites that must be satisfied before you can run this workflow
"How this Workflow Works" on page 163	Information about what the workflow does, including validation checks performed, steps executed, and a high-level process flow
"How to Run this Workflow" on page 167	Instructions for running this workflow in your environment
"Parameters for DB2 - Offline HADR Rollback Fixpack" on page 170	List of input parameters for this workflow

Prerequisites

Before performing the procedures in this section, your environment must meet the following minimum requirements:

- A server running AIX 6.1 or 7.1 or Red Hat Enterprise Linux 5 or 6. The operating system platform must be certified for the pertinent DB2 fix pack version.
- DB2 server software—version 9.5, 9.7, 10.1, or 10.5—is installed on the target and is ready to be patched.
- The infrastructure required for applying the fix pack is in place.
- All DB2 Instances are on the same initial fix pack version.
- Patch media:

The DB2 server fix pack file from IBM.

Patch installation files must be available locally or available for download from the software repository.

- Storage: A staging directory with 7-8 gigabytes available to unpack the binary file and to apply the fix pack and archive—requires about double the size of the current DB2 installation on the disk. By default, it is expected to have about double the size of current DB2 Installation on the disk.
- The operating system platform is certified for the pertinent DB2 specific fixpack version.
- The operating system kernel parameters and virtual and shared memory are properly configured to avoid any failure while applying the DB2 fix pack.
- License for DMA.
- License for DB2 Database version 9.5, 9.7, 10.1, or 10.5.
- The workflow must have the unchallenged ability to become the OS administrator user (typically root on UNIX systems).
- For all the instances on the target server, the license has to be activated to use; otherwise the workflow will not be able to restart the instances after the fixpack is applied and database connection may not be possible again.
- The user who runs the workflow with the server wrapper must have the access to create or modify the directory structure for instances and databases.
- All the DMA database metadata must be up-to-date on the target server where the workflow is deployed.

- If an instance update fails, you must manually bind the packages (for each database) using the command **DB2DIR/instance/db2iupdt** *instance name*.
- If DB2 admin server is installed and the update fails during fixpack, you must manually update the DB2 admin server by using the following commands:
 - **DB2DIR/instance/dasupdt** and start up the DB2 admin server by using **su - instance name** and **db2admin start** commands
- If the database uses federation, perform the following additional binds:
 - **db2 BIND INSTHOME\sqllib\bnd\db2dsproc.bnd** blocking all grant public
 - **db2 BIND INSTHOME\sqllib\bnd\db2stats.bnd** blocking all grant public

Additional requirements

For additional requirements, see the following IBM documentation:

DB2 version	IBM documentation
9.5	DB2 Version 9.5 Fix Pack
9.7	DB2 Version 9.7 Fix Pack
10.1	DB2 Version 10.1 Fix Pack
10.5	DB2 Version 10.5 Fix Pack

How this Workflow Works

The following information describes how the DB2 - Offline HADR Rollback Fixpack workflow works:

Overview

This workflow does the following things in the order shown:

- First, the workflow prepares to rollback the patch. It prepares the server, determines the DB2 home, prepares the DB2 instance, and validates the input parameters. If the fixpack files do not already exist they are downloaded from SA. It determines all the pertinent fixpack information.
- Offline HADR software archives are staged, database configuration is backed up, and DB2 instances are shutdown.
- Fixpack is rolled back for offline HADR installation and DB2 instances are updated.
- The workflow verifies the fixpack.
- The DB2 instances are restarted and packages are bound to the databases.
- The DB2 databases are discovered.
- Finally, the workflow cleans up files that are no longer needed.

Validation Checks Performed

Much of the validation centers on the input parameters:

- The input parameters have the proper syntax (no special characters or spaces).
- Files exist or have valid specifications.
- The supplied fixpack update applies to the current version.

Workflow Steps

Steps Used in DB2 - Offline HADR Apply Fixpack

Workflow Step	Description
Gather Parameters to Patch Offline HADR Fixpack	This step accepts parameters for the workflow. All the parameters are mandatory in this step.
Gather Advanced Parameters to Patch Offline HADR Fixpack	This step sets all the DB2 advanced configurable parameters that are used in subsequent workflow steps.
Validate Parameters for Patch Offline HADR Fixpack	This step validates all the input parameter values received, validates the DB2 target, and ensures it meets all the criteria to rollback fixpack.
Stage Offline HADR Fixpack Software Archive	This step validates the input staging path and binary archive files to unpack (unzip or extract) to install the software. Depending upon the file extensions(.tar, .gz), it chooses the right library to unpack the software binary file. It also validates the disk space availability before it unpacks the binary file.
Download Software	This step automates the transfer of files from the HPE SA software library to individual managed servers for use in downstream workflow steps. Verifies checksum of each file transferred.
Capture Configuration and take full Offline Backup	This step capture various configuration details of DB2 database on the target. It also takes the offline database backup of the database.
Shutdown DB2 Instances For Offline HADR Rollback	This step shuts down the DB2 processes like DAS, fault monitor, and licensing daemon before rolling back the fixpack.
DeInstall DB2 Fixpack To Offline HADR Installation	This step runs the installFixpack utility from DB2 and rolls back the fixpack using the -f level parameter of installFixPack command for the existing DB2 Installation. As part of installFixpack run, it also updates all the instances against the DB2 installation which are patched. It does not update any database on the fixpack level that we applied. That has to be performed manually for all the databases that are created under the instances that have been patched.
Update DB2 Instances For Offline HADR	This step scans the target server and discovers all the instances eligible to update with the newly installed fixpack. It will then update each instance(s) with the new fixpack installation pointing to it.
Restore to Original State	<p>This step restores the installation to its previous state. The restore is at 3 stages:</p> <ol style="list-style-type: none"> 1. Installation 2. Instance 3. Database using restore from backup <p>This step runs the installFixPack command at the location where Current Fixpack Archive is unpacked to revert the fixpack to its original state.</p>
Verify Offline HADR Patch	This steps runs the db2level utility from DB2 and to verifies if the

Steps Used in DB2 - Offline HADR Apply Fixpack , continued

Workflow Step	Description
Fixpack	existing DB2 installation is on the same fixpack level that is applied in this workflow. It also verifies if all the instances provided against the DB2 installation location are also on the same patch level as expected.
Discover DB2 Databases	<p>This step audits the server's physical environment looking for DB2 databases.</p> <p>Discovery is only additive. It will not remove instances or databases currently in your environment. It is the end-user's responsibility to delete content that is no longer in use.</p> <p>In cluster situations where one node is active while other nodes are inactive, Discovery will only find instances and databases on the active node. Nothing will be added to inactive nodes.</p>
Restart DB2 Instances For Fixpack	This step restarts all the DB2 instances and processes provisioned against the user specified input DB2 installation location.
Cleanup Downloaded Files	This step removes files and archives that were downloaded to the target system during previous workflow steps.
Bind Packages To Database	This step binds various packages to database(s) for each instance(s) created against current DB2 installation. The default value is set to "false" which will not bind any packages. If it is set to "true", binding will occur for all the database eligible for new package bindings post applying the fixpack. By doing this, databases can use the features of newly applied fixpack.

For parameter descriptions and defaults, see ["Parameters for DB2 - Offline HADR Rollback Fixpack" on page 170](#).

How to Run this Workflow

The following instructions show you how to customize and run the DB2 - Offline HADR Apply Fixpack workflow in your environment.

The workflow provides default values for some parameters. These default values are usually sufficient for a "typical" installation. You can override the defaults by specifying parameter values in the deployment. You can also expose additional parameters in the workflow, if necessary, to accomplish more advanced scenarios. Any parameters not explicitly specified in the deployment will have the default values listed in ["Parameters for DB2 - Offline HADR Rollback Fixpack" on page 170](#).

Note: Before following this procedure, review the ["Prerequisites" on page 162](#), and ensure that all requirements are satisfied.

To use the the DB2 - Offline HADR Apply Fixpack workflow:

1. Create a deployable copy of the workflow.
2. Determine the values that you will specify for the following parameters:

Input parameters in the step: Gather Parameters to Patch Offline HADR Fixpack

Parameter Name	Default Value	Required	Description
Current Fixpack Archive	no default	required	Fully qualified file name of DB2 fixpack archive which is currently applied to the DB2 Installation.
DB2 Installation Location	no default	required	Fully qualified path where DB2 is installed on the target server.
Required Fixpack Archive	no default	required	Fully qualified file name of DB2 fixpack archive which is intended to be applied to the DB2 Installation.

Input parameters in the step: Gather Advanced Parameters to Patch Offline HADR Fixpack

Parameter Name	Default Value	Required	Description
Clean on Success	True	optional	Determines whether to remove downloaded and extracted files as well as cleans up installed directory on successful execution of workflow. Default is set to True, which will clean up on failure.
DB2 Installation Location	no default	required	Fully qualified path where DB2 is installed on the target server.
Download Location	/tmp/archive	optional	Fully qualified directory path

Input parameters in the step: Gather Advanced Parameters to Patch Offline HADR Fixpack, continued

Parameter Name	Default Value	Required	Description
			where the user specified fixpack file will be downloaded to use it for applying fixpack.
Fixpack Install Folder	no default	optional	The folder where the fixpack will be installed. If left blank, it will be installed on the DB2 installation.
Offline Backup Location	no default	optional	Fully qualified path where the offline database backup will be stored on the target server. Please note that the path should have requisite permissions so it can be accessible from all DB2 instances.
Rebind Packages To Database	False	optional	Flag to enable or disable binding capability of workflow step for various packages to database(s) for each instance(s) created against current DB2 installation. The default value is set to "false" which will not bind any packages. Valid values are "yes", "y", "true", "false", "n", or "no".
Staging Directory	/tmp/staging	optional	Fully qualified path of the directory where DB2 installer will be extracted from archive. Will be cleaned up at end of workflow execution. Default value is /tmp/staging.
Instance SSL Port	no default	optional	Comma separated list of values corresponding to an instance name. This will be used to initialize the listener port in the SSL configuration file. For example, if Instance Name Parameter value is http_instance1,http_instance2, the port values can be 1234,4321 where 1234 belongs to http_instance1 and 4321 belongs to http_instance2.
Web Service Password	no default	optional	Password for the DMA Discovery web service API to discover and update the metadata in DMA.
Web Service URL	no default	optional	URL for the DMA Discovery web service API to discover and

Input parameters in the step: Gather Advanced Parameters to Patch Offline HADR Fix-pack, continued

Parameter Name	Default Value	Required	Description
			update metadata in DMA.
Web Service User	no default	optional	User for the DMA Discovery web service API to discover and update metadata in DMA.

Note: See ["Parameters for DB2 - Offline HADR Rollback Fixpack" on the next page](#) for detailed descriptions of all input parameters for this workflow, including default values.

3. In the workflow editor, expose any additional parameters that you need . You will specify values for those parameters when you create the deployment.
4. Save the changes to the workflow (click **Save** in the lower right corner).
5. Create a new deployment.
6. On the Parameters tab, specify values for the required parameters listed in step 2 and any additional parameters that you have exposed. You do not need to specify values for those parameters whose default values are appropriate for your environment.
7. On the Targets tab, specify one or more targets for this deployment.

Note: The target for this workflow is an instance.

8. Save the deployment (click **Save** in the lower right corner).
9. Run the workflow using this deployment.

To verify the results:

The workflow will complete and report SUCCESS on the Console if it has run successfully. If an error occurs during workflow execution, the error is logged, and the workflow terminates in the FAILURE state.

Parameters for DB2 - Offline HADR Rollback Fixpack

The following tables describe the required and optional input parameters for this workflow. Several of these parameters are not initially visible in a deployment. For many parameters, if you do not specify a value for a parameter, a default value is assigned.

Parameters in the step: Gather Parameters to Patch Offline HADR Fixpack

Parameter Name	Default Value	Required	Example Value	Description
Current Fixpack Archive	no default	required	v10.1fp2_linuxx64_server.tar.gz	Fully qualified file name of DB2 fixpack archive which is currently applied to the DB2 Installation.
DB2 Installation Location	no default	required	/opt/ibm/db2/V10.5	Fully qualified path where DB2 is installed on the target server.
Required Fixpack Archive	no default	required	v10.1fp3_linuxx64_server.tar.gz	Fully qualified file name of DB2 fixpack archive which is intended to be applied to the DB2 Installation.

Parameters in the step: Gather Advanced Parameters to Patch Offline HADR Fixpack

Parameter Name	Default Value	Required	Example Value	Description
Clean on Success	True	optional	True	Determines whether to remove downloaded and extracted files as well as cleans up installed directory on successful execution of workflow. Default is set to True, which will clean up on failure.
DB2 Installation Location	no default	required	/opt/ibm/db2/V10.5	Fully qualified path where DB2 is installed on the target server.
Download Location	/tmp/archive	optional	/tmp/archive	Fully qualified directory path where the user specified fixpack file will be downloaded to use it for applying fixpack.
Fixpack Install Folder	no default	optional	/opt/ibm/db2/V10.5/fp2	The folder where the fixpack will be installed. If left blank, it will be installed on the DB2 installation.
Offline Backup Location	no default	optional	/tmp/backup	Fully qualified path where the offline database backup will be stored on the target server. Please note that the path should have requisite

Parameters in the step: Gather Advanced Parameters to Patch Offline HADR Fixpack, continued

Parameter Name	Default Value	Required	Example Value	Description
				permissions so it can be accessible from all DB2 instances.
Rebind Packages To Database	False	optional	False	Flag to enable or disable binding capability of workflow step for various packages to database(s) for each instance(s) created against current DB2 installation. The default value is set to "false" which will not bind any packages. Valid values are "yes", "y", "true", "false", "n", or "no".
Staging Directory	/tmp/staging	optional	/tmp/staging	Fully qualified path of the directory where DB2 installer will be extracted from archive. Will be cleaned up at end of workflow execution. Default value is /tmp/staging.
Instance SSL Port	no default	optional		Comma separated list of values corresponding to an instance name. This will be used to initialize the listener port in the SSL configuration file. For example, if Instance Name Parameter value is http_instance1,http_instance2, the port values can be 1234,4321 where 1234 belongs to http_instance1 and 4321 belongs to http_instance2.
Web Service Password	no default	optional		Password for the DMA Discovery web service API to discover and update the metadata in DMA.
Web Service URL	no default	optional		URL for the DMA Discovery web service API to discover and update metadata in DMA.
Web Service User	no default	optional		User for the DMA Discovery web service API to discover and update metadata in DMA.

DB2 - Rollback Helper

This workflow is used for rolling back fixpacks on an offline DB2 HADR installation. This workflow is invoked from within the parent workflow, ["DB2 - Offline HADR Fixpack Parent Flow v3" on page 142](#).

This workflow rolls back fixpack for IBM DB2 LUW (Linux, UNIX, and Windows) instances on the target server. It currently supports the DB2 Versions 9.5, 9.7, 10.1, 10.5 on Red Hat Linux and AIX servers. This is a server level workflow. It will rollback the fixpack to the DB2 Home (also known as the DB2 installation directory, for example: /opt/ibm/db2/V10.5) installed on the target machine where this workflow is deployed. It updates all the instances with the fixpack of DB2 that are created against the specific DB2 installation.

This workflow shuts down all the DB2 instances, DB2 Admin Server, and licensing daemons that are running for all the instances that are provisioned against a specific DB2 home (DB2 Installation Location). It kills all the application user connections with DB2 instances that are to be patched. It validates the eligibility for the fixpack to apply by comparing the current fixpack level on the installed DB2 against the fixpack level that user is trying to apply.

To use this workflow in your environment, see the following information:

Topic	Information Included
"Prerequisites" below	List of prerequisites that must be satisfied before you can run this workflow
"How this Workflow Works" on page 174	Information about what the workflow does, including validation checks performed, steps executed, and a high-level process flow
"How to Run this Workflow" on page 176	Instructions for running this workflow in your environment
"Parameters for DB2 - Rollback Helper" on page 179	List of input parameters for this workflow

Prerequisites

Before performing the procedures in this section, your environment must meet the following minimum requirements:

- To use this workflow, you must provide the DB2 fixpack archive file which is downloaded either on the target server, or where it can be downloaded by the workflow.
- The workflow must have the unchallenged ability to become the OS administrator user (typically root on UNIX systems).

- For all the instances on the target machine, the license has to be activated to use; otherwise the workflow will not be able to restart the instances after the fixpack is applied and database connection may not be possible again.
- The user who runs the workflow with the server wrapper must have the access to create or modify the directory structure for instances and databases.
- As stated in the IBM DB2 release bulletin, the following prerequisites must be satisfied before this workflow is run:
 - DB2 software must be already installed on the target machine.
 - The infrastructure required for applying fixpack should be in place. Make sure the target server has adequate available disk space to unpack the binary file and apply the fixpack. By default, it is expected to have about double the size of current DB2 Installation on the disk.
 - The operating system platform is certified for the pertinent DB2 specific fixpack version.
 - The operating system kernel parameters and virtual and shared memory is properly configured to avoid any failure while applying the DB2 fixpack.
- All DMA database metadata must be up-to-date on the target server where the workflow is deployed.
- The workflow currently applies the fixpack to all the instances against the specific DB2 Installation. It does not currently support to apply the fixpack for a specific instance.
- If an instance update fails, you must manually bind the packages (for each database) using the command **DB2DIR/instance/db2iupdt***instance name*.
- If DB2 admin server is installed and the update fails during fixpack, you must manually update the DB2 admin server by using the following commands:
 - **DB2DIR/instance/dasupdt** and start up the DB2 admin server by using **su - instance name** and **db2admin start** commands
- If the database uses federation, perform the following additional binds:
 - **db2 BIND INSTHOME\sqllib\bnd\db2dsproc.bnd** blocking all grant public
 - **db2 BIND INSTHOME\sqllib\bnd\db2stats.bnd** blocking all grant public

Additional requirements

For additional requirements, see the following IBM documentation:

DB2 version	IBM documentation
9.5	DB2 Version 9.5 Fix Pack
9.7	DB2 Version 9.7 Fix Pack

DB2 version	IBM documentation
10.1	DB2 Version 10.1 Fix Pack
10.5	DB2 Version 10.5 Fix Pack

How this Workflow Works

The following information describes how the DB2 - Rollback Helper workflow works:

Overview

This workflow does the following things in the order shown:

- First, the workflow prepares to rollback the patch. It prepares the server, determines the DB2 home, prepares the DB2 instance, and validates the input parameters. If the fixpack files do not already exist they are downloaded from SA. It determines all the pertinent fixpack information.
- Fixpack binries are staged and DB2 instances are shutdown.
- Fixpack is rolled back and DB2 instances are updated.
- The workflow verifies the fixpack.
- The DB2 instances are restarted and packages are bound to the databases.
- The DB2 databases are discovered.
- Finally, the workflow cleans up files that are no longer needed.

Validation Checks Performed

Much of the validation centers on the input parameters:

- The input parameters have the proper syntax (no special characters or spaces).
- Files exist or have valid specifications.
- The supplied fixpack update applies to the current version.

Workflow Steps

Steps Used in DB2 - Rollback Helper

Workflow Step	Description
Gather Parameters to Patch Offline HADR Fixpack	This step accepts parameters for the workflow. All the parameters are mandatory in this step.
Gather Advanced Parameters to Patch Offline HADR Fixpack	This step sets all the DB2 advanced configurable parameters that are used in subsequent workflow steps.
Prepare Binaries List	This step accepts the current and required fixpack binaries and formats them.
Shutdown DB2 Instances For Rollback	This step shuts down the DB2 processes like DAS, fault monitor, and licensing daemon before rolling back the fixpack.
DeInstall DB2 Fixpack in Rollback	This step runs the installFixpack utility from DB2 and rolls back the fixpack using the -f level parameter of installFixPack command for the existing DB2 Installation. As part of installFixpack run, it also updates all the instances against the DB2 installation which are patched. It does not update any database on the fixpack level that we applied. That has to be performed manually for all the databases that are created under the instances that have been patched.
Update DB2 Instances For Offline HADR	This step scans the target server and discovers all the instances eligible to update with the newly installed fixpack. It will then update each instance(s) with the new fixpack installation pointing to it.
Verify Offline HADR Patch Fixpack	This steps runs the db2level utility from DB2 and to verifies if the existing DB2 installation is on the same fixpack level that is applied in this workflow. It also verifies if all the instances provided against the DB2 installation location are also on the same patch level as expected.
Restart DB2 Instances For Fixpack	This step restarts all the DB2 instances and processes provisioned against the user specified input DB2 installation location.
Discover DB2 Databases	<p>This step audits the server's physical environment looking for DB2 databases.</p> <p>Discovery is only additive. It will not remove instances or databases currently in your environment. It is the end-user's responsibility to delete content that is no longer in use.</p> <p>In cluster situations where one node is active while other nodes are inactive, Discovery will only find instances and databases on the active node. Nothing will be added to inactive nodes.</p>
Cleanup Downloaded Files	This step removes files and archives that were downloaded to the target system during previous workflow steps.

For parameter descriptions and defaults, see ["Parameters for DB2 - Rollback Helper" on page 179](#).

How to Run this Workflow

The following instructions show you how to customize and run the DB2 - Rollback Helper workflow in your environment.

The workflow provides default values for some parameters. These default values are usually sufficient for a "typical" installation. You can override the defaults by specifying parameter values in the deployment. You can also expose additional parameters in the workflow, if necessary, to accomplish more advanced scenarios. Any parameters not explicitly specified in the deployment will have the default values listed in ["Parameters for DB2 - Rollback Helper" on page 179](#).

Note: Before following this procedure, review the ["Prerequisites" on page 172](#), and ensure that all requirements are satisfied.

To use the the DB2 - Offline HADR Apply Fixpack workflow:

1. Create a deployable copy of the workflow.
2. Determine the values that you will specify for the following parameters:

Input parameters in the step: Gather Parameters to Patch Offline HADR Fixpack

Parameter Name	Default Value	Required	Description
Current Fixpack Archive	no default	required	Fully qualified file name of DB2 fixpack archive which is currently applied to the DB2 Installation.
DB2 Installation Location	no default	required	Fully qualified path where DB2 is installed on the target server.
Required Fixpack Archive	no default	required	Fully qualified file name of DB2 fixpack archive which is intended to be applied to the DB2 Installation.

Input parameters in the step: Gather Advanced Parameters to Patch Offline HADR Fixpack

Parameter Name	Default Value	Required	Description
Clean on Success	True	optional	Determines whether to remove downloaded and extracted files as well as cleans up installed directory on successful execution of workflow. Default is set to True, which will clean up on failure.
DB2 Installation Location	no default	required	Fully qualified path where DB2 is installed on the target server.
Download Location	/tmp/archive	optional	Fully qualified directory path

Input parameters in the step: Gather Advanced Parameters to Patch Offline HADR Fixpack, continued

Parameter Name	Default Value	Required	Description
			where the user specified fixpack file will be downloaded to use it for applying fixpack.
Fixpack Install Folder	no default	optional	The folder where the fixpack will be installed. If left blank, it will be installed on the DB2 installation.
Offline Backup Location	no default	optional	Fully qualified path where the offline database backup will be stored on the target server. Please note that the path should have requisite permissions so it can be accessible from all DB2 instances.
Rebind Packages To Database	False	optional	Flag to enable or disable binding capability of workflow step for various packages to database(s) for each instance(s) created against current DB2 installation. The default value is set to "false" which will not bind any packages. Valid values are "yes", "y", "true", "false", "n", or "no".
Staging Directory	/tmp/staging	optional	Fully qualified path of the directory where DB2 installer will be extracted from archive. Will be cleaned up at end of workflow execution. Default value is /tmp/staging.
Instance SSL Port	no default	optional	Comma separated list of values corresponding to an instance name. This will be used to initialize the listener port in the SSL configuration file. For example, if Instance Name Parameter value is http_instance1,http_instance2, the port values can be 1234,4321 where 1234 belongs to http_instance1 and 4321 belongs to http_instance2.
Web Service Password	no default	optional	Password for the DMA Discovery web service API to discover and update the metadata in DMA.
Web Service URL	no default	optional	URL for the DMA Discovery web service API to discover and

Input parameters in the step: Gather Advanced Parameters to Patch Offline HADR Fix-pack, continued

Parameter Name	Default Value	Required	Description
			update metadata in DMA.
Web Service User	no default	optional	User for the DMA Discovery web service API to discover and update metadata in DMA.

Note: See ["Parameters for DB2 - Rollback Helper" on the next page](#) for detailed descriptions of all input parameters for this workflow, including default values.

3. In the workflow editor, expose any additional parameters that you need . You will specify values for those parameters when you create the deployment.
4. Save the changes to the workflow (click **Save** in the lower right corner).
5. Create a new deployment.
6. On the Parameters tab, specify values for the required parameters listed in step 2 and any additional parameters that you have exposed. You do not need to specify values for those parameters whose default values are appropriate for your environment.
7. On the Targets tab, specify one or more targets for this deployment.

Note: The target for this workflow is an instance.

8. Save the deployment (click **Save** in the lower right corner).
9. Run the workflow using this deployment.

To verify the results:

The workflow will complete and report SUCCESS on the Console if it has run successfully. If an error occurs during workflow execution, the error is logged, and the workflow terminates in the FAILURE state.

Parameters for DB2 - Rollback Helper

The following tables describe the required and optional input parameters for this workflow. Several of these parameters are not initially visible in a deployment. For many parameters, if you do not specify a value for a parameter, a default value is assigned.

Parameters in the step: Gather Parameters to Patch Offline HADR Fixpack

Parameter Name	Default Value	Required	Example Value	Description
Current Fixpack Archive	no default	required	v10.1fp2_linuxx64_server.tar.gz	Fully qualified file name of DB2 fixpack archive which is currently applied to the DB2 Installation.
DB2 Installation Location	no default	required	/opt/ibm/db2/V10.5	Fully qualified path where DB2 is installed on the target server.
Required Fixpack Archive	no default	required	v10.1fp3_linuxx64_server.tar.gz	Fully qualified file name of DB2 fixpack archive which is intended to be applied to the DB2 Installation.

Parameters in the step: Gather Advanced Parameters to Patch Offline HADR Fixpack

Parameter Name	Default Value	Required	Example Value	Description
Clean on Success	True	optional	True	Determines whether to remove downloaded and extracted files as well as cleans up installed directory on successful execution of workflow. Default is set to True, which will clean up on failure.
DB2 Installation Location	no default	required	/opt/ibm/db2/V10.5	Fully qualified path where DB2 is installed on the target server.
Download Location	/tmp/archive	optional	/tmp/archive	Fully qualified directory path where the user specified fixpack file will be downloaded to use it for applying fixpack.
Offline Backup Location	no default	optional	/tmp/backup	Fully qualified path where the offline database backup will be stored on the target server. Please note that the path should have requisite permissions so it can be accessible from all DB2 instances.
Rebind Packages To Database	False	optional	False	Flag to enable or disable binding capability of workflow

Parameters in the step: Gather Advanced Parameters to Patch Offline HADR Fixpack, continued

Parameter Name	Default Value	Required	Example Value	Description
				step for various packages to database(s) for each instance (s) created against current DB2 installation. The default value is set to "false" which will not bind any packages. Valid values are "yes", "y", "true", "false", "n", or "no".
Staging Directory	/tmp/staging	optional	/tmp/staging	Fully qualified path of the directory where DB2 installer will be extracted from archive. Will be cleaned up at end of workflow execution. Default value is /tmp/staging.
Web Service Password	no default	optional		Password for the DMA Discovery web service API to discover and update the metadata in DMA.
Web Service URL	no default	optional		URL for the DMA Discovery web service API to discover and update metadata in DMA.
Web Service User	no default	optional		User for the DMA Discovery web service API to discover and update metadata in DMA.

DB2 - Fixpack Validator v2

This section describes how to use DMA to create a repeatable, standardized method to quickly and accurately apply IBM DB2 fixpack for DB2 installations across an enterprise to keep fix packs current.

This workflow is a wrapper or parent workflow which launches subflows to validate and apply fixpacks on a DB2 Installation. A deployment of this workflow has to be created and appropriate values have to be provided. These deployment values will be automatically passed on to the subflows that this workflow triggers.

To use this workflow in your environment, see the following information:

Topic	Information Included
"Prerequisites" below	List of prerequisites that must be satisfied before you can run this workflow
"How this Workflow Works" on the next page	Information about what the workflow does, including validation checks performed, steps executed, and a high-level process flow
"How to Run this Workflow" on page 184	Instructions for running this workflow in your environment
"Parameters for DB2 - Fixpack Validator" on page 186	List of input parameters for this workflow

Prerequisites

Before performing the procedures in this section, your environment must meet the following minimum requirements:

- A server running AIX 6.1 or 7.1 or Red Hat Enterprise Linux 5 or 6. The operating system platform must be certified for the pertinent DB2 fix pack version.
- DB2 server software—version 9.5, 9.7, 10.1, or 10.5—is installed on the target and is ready to be patched.
- The infrastructure required for applying the fix pack is in place.
- All DB2 Instances are on the same initial fix pack version.
- Patch media:

The DB2 server fix pack file from IBM.

Patch installation files must be available locally or available for download from the software repository.

Note: DMA only applies DB2 server fix packs, not universal fix packs.

- Storage: A staging directory with 7-8 gigabytes available to unpack the binary file and to apply the fix pack and archive—requires about double the size of the current DB2 installation on the disk. By default, it is expected to have about double the size of current DB2 Installation on the disk.
- The operating system platform is certified for the pertinent DB2 specific fixpack version.
- The operating system kernel parameters and virtual and shared memory are properly configured to avoid any failure while applying the DB2 fix pack.

- License for DMA.
- License for DB2 Database version 9.5, 9.7, 10.1, or 10.5.
- The workflow must have the unchallenged ability to become the OS administrator user (typically root on UNIX systems).
- For all the instances on the target server, the license has to be activated to use; otherwise the workflow will not be able to restart the instances after the fixpack is applied and database connection may not be possible again.
- The user who runs the workflow with the server wrapper must have the access to create or modify the directory structure for instances and databases.
- All the DMA database metadata must be up-to-date on the target server where the workflow is deployed.

Additional requirements

For additional requirements, see the following IBM documentation:

DB2 version	IBM documentation
9.5	DB2 Version 9.5 Fix Pack
9.7	DB2 Version 9.7 Fix Pack
10.1	DB2 Version 10.1 Fix Pack
10.5	DB2 Version 10.5 Fix Pack

How this Workflow Works

The following information describes how DB2 - Fixpack Validator workflow works:

Overview

This workflow does the following things in the order shown:

- First, the workflow prepares to validate the patch. It determines the DB2 home, staging directory, checks for existing and checks for required fixpack archives, and validates the input parameters. If the fixpack files do not already exist they are downloaded. It determines all the pertinent fixpack information.
- The workflow prepares the staging directory by unpacking (unzipping or extracting) binary archive file and transfers files from the HPE SA software library to individual managed servers for use in downstream workflow steps.
- Finally, validates fixpack binary levels of the current and required fixpack files.

Validation Checks Performed

Much of the validation centers on the input parameters:

- The input parameters have the proper syntax (no special characters or spaces).
- Files exist or have valid specifications.
- The supplied fixpack update applies to the current version.

Workflow Steps

Steps Used in DB2 - Fixpack Validator

Workflow Step	Description
Gather Parameters To Validate Patch Fixpack v2	This step accepts parameters for the workflow. All the parameters are mandatory in this step.
Validate Parameters for Patch Fixpack Validator	This step validates all the input parameter values received in the gather input parameters step, validates the DB2 target, and make sure it meets all the criteria to apply fixpack.
Stage Offline HADR Fixpack Software Archive	This step validates the input staging path and binary archive file to unpack (unzip or extract) to install the software. Depending upon the file extensions (.tar or .gz), it chooses the right library to unpack the software binary file. It also validates the disk space availability before it unpacks the binary file.
Download Software	This step automates the transfer of files from the HPE SA Software Library to individual managed servers for use in downstream workflow steps. It also verifies checksum of each file transferred.
Validate Fixpack Binaries and Level v2	This step validates the fixpack level of the current DB2 installation with the fixpack level of the required fixpack binary file.

For parameter descriptions and defaults, see ["Parameters for DB2 - Fixpack Validator" on page 186](#).

How to Run this Workflow

The following instructions show you how to customize and run the DB2 - Offline HADR Fixpack Parent Flow workflow in your environment.

The workflow provides default values for some parameters. These default values are usually sufficient for a "typical" installation. You can override the defaults by specifying parameter values in the deployment. You can also expose additional parameters in the workflow, if necessary, to accomplish more advanced scenarios. Any parameters not explicitly specified in the deployment will have the default values listed in ["Parameters for DB2 - Fixpack Validator" on page 186](#).

Note: Before following this procedure, review the ["Prerequisites" on page 181](#), and ensure that all requirements are satisfied.

To use the DB2 - Offline HADR Fixpack Parent Flow workflow:

1. Create a deployable copy of the workflow.
2. Determine the values that you will specify for the following parameters:

Input parameters in the step: Gather Parameters Patch Fixpack Offline HADR In Parent

Parameter Name	Default Value	Required	Description
Current Fixpack Archive	no default	required	Fully qualified file name of the required fixpack archive that will be applied.
DB2 Installation Location	no default	required	Fully qualified path where DB2 is installed on the target server.
Download Location	/tmp	required	Fully qualified directory path where the user specified fixpack file will be downloaded.
Required Fixpack Archive	no default	required	Fully qualified file name of the required fixpack archive that will be applied.
Staging Directory	no default	required	Fully qualified path of the directory where DB2 installer will be extracted from archive.

Note: See ["Parameters for DB2 - Fixpack Validator" on page 186](#) for detailed descriptions of all input parameters for this workflow, including default values.

3. In the workflow editor, expose any additional parameters that you need . You will specify values for those parameters when you create the deployment.
4. Save the changes to the workflow (click **Save** in the lower right corner).
5. Create a new deployment.

6. On the Parameters tab, specify values for the required parameters listed in step 2 and any additional parameters that you have exposed. You do not need to specify values for those parameters whose default values are appropriate for your environment.
7. On the Targets tab, specify one or more targets for this deployment.

Note: The target for this workflow is an instance.

8. Save the deployment (click **Save** in the lower right corner).
9. Run the workflow using this deployment.

To verify the results:

The workflow will complete and report SUCCESS on the Console if it has run successfully. If an error occurs during workflow execution, the error is logged, and the workflow terminates in the FAILURE state.

Parameters for DB2 - Fixpack Validator

The following tables describe the required and optional input parameters for this workflow. Several of these parameters are not initially visible in a deployment.

Parameters in the step: Gather Parameters To Validate Patch Fixpack v2

Parameter Name	Default Value	Required	Example Value	Description
Current Fixpack Archive	no default	required	v10.1fp4_linuxx64_server.tar.gz	Fully qualified file name of the required fixpack archive that will be applied.
DB2 Installation Location	no default	required	opt/ibm/db2/V10.5	Fully qualified path where DB2 is installed on the target server.
Download Location	/tmp	required	/tmp	Fully qualified directory path where the user specified fixpack file will be downloaded.
Required Fixpack Archive	no default	required	v10.1fp4_linuxx64_server.tar.gz	Fully qualified file name of the required fixpack archive that will be applied.
Staging Directory	no default	required		Fully qualified path of the directory where DB2 installer will be extracted from archive.

DB2 - Upgrade Instance and Database

This workflow upgrades DB2 instance(s) and database(s) for IBM DB2 LUW (Linux, UNIX, and Windows) on the target server where this workflow is deployed. It currently supports the DB2 Versions 9.5, 9.7, 10.1, 10.5 on Red Hat Linux and AIX servers. This is a server level workflow. It will install the software and upgrade the existing DB2 Home (also known as the DB2 Installation Directory, for example: /opt/ibm/db2/V10.5) installed on the target machine where this workflow is deployed. It upgrades all instances and databases that exist for each respective DB2 setup.

This workflow supports the following upgrade use cases:

- DB2 9.5 to 9.7
- DB2 9.5 to 10.1
- DB2 9.7 to 10.1

- DB2 9.7 to 10.5
- DB2 10.1 to 10.5

This workflow shuts down all DB2 instances, DB2 Admin Server, and licensing daemons that are running for all the instances that are provisioned against a specific DB2 home (DB2 Installation Location). It kills all application user connections with DB2 instances that are to be upgraded. It validates the eligibility for the instance(s) and database(s) to be upgraded by comparing the current DB2 installation or fixpack level on the installed DB2 against the DB2 installation or fixpack level that user desires to upgrade to.

Note: This workflow support DB2 version 10.1 or 10.5 on a Red Hat Linux or AIX server.

Before running the DB2 - Upgrade Instance and Database workflow, the DB2 license must be activated for the instances that you create.

To use this workflow in your environment, see the following information:

Topic	Information Included
"Prerequisites" below	List of prerequisites that must be satisfied before you can run this workflow
"How this Workflow Works" on the next page	Information about what the workflow does, including validation checks performed, steps executed, and step descriptions
"How to Run this Workflow" on page 190	Instructions for running this workflow in your environment
"Parameters for DB2 - Upgrade Instance and Database" on page 194	List of input parameters for this workflow

Prerequisites

Before performing the procedures in this section, your environment must meet the following minimum requirements:

- A server running one of the following operating systems (any version that is supported by IBM DB2 and DMA):
 - Linux
 - AIX

See the *DMA Support Matrix* for specific operating system versions, available at:

<http://hpln.hp.com/group/database-and-middleware-automation>.

- Installation media:

The DB2 server installation software binary file from IBM.

Installation software binary file must be available locally or available for download from the software repository.

- DB2 software must already be installed on the target server.
- Target server has available disk space to unpack the binary file and apply fixpack.
- Unchallenged ability to become the OS administrator user (typically root on UNIX systems).
- The following workflow requirements:

Workflow	Requirements
DB2 - Upgrade Instance and Database	<p>The user who runs the workflow with the server wrapper must have access to create or modify the directory structure for instances and databases.</p> <p>After creating the instances, the license must be activated before the database can use the instance.</p> <p>The DMA database metadata is up-to-date for the DB2 Instance where the workflow is deployed.</p>

Refer to the [IBM Documentation](#) for the following:

- Complete installation and infrastructure requirements for IBM DB2.
- Acceptable types and range of values when using DMA advanced parameters to configure IBM DB2 settings.

How this Workflow Works

This workflow performs the following actions:

Upgrades DB2 instances and databases.

Steps Executed

The DB2 - Upgrade Instance and Database workflow includes the following steps. Each step must complete successfully before the next step can start. If a step fails, the workflow reports a failure and all subsequent steps are skipped.

Steps Used by DB2 - Upgrade Instance and Database

Workflow Step	Description
Gather Parameters for	This step accepts input parameters for the workflow.

Steps Used by DB2 - Upgrade Instance and Database , continued

Workflow Step	Description
DB2 Upgrade Instance and Database	
Gather Advanced Parameters for DB2 Upgrade Instance and Database	This step accepts optional parameter values for the workflow.
Validate Parameters for DB2 Upgrade Instance and Database	This step validates all the input parameter values received in the gather and advanced gather input parameters steps, validate the DB2 target, and makes sure it meets all the necessary criteria to start the upgrade process.
Stage DB2 Software Archive	This step uncompresses the archive file if compressed and then extracts the files from it (tar file) under staging path.
Download Software	This step automates the transfer of files from the HPE SA Software Library to individual managed servers for use in downstream workflow steps. Verifies checksum of each file transferred.
Install DB2 Software to Upgrade Instance and Database	This step installs DB2 Software on the specified location specified in the input parameter.
Cleanup Failed DB2 Upgrade	This step removes files and archives that were downloaded to the target system during previous workflow steps.
Configure DB2 Upgrade Permissions	This step checks for the permission level of the existing DB2 installation for the users and groups and migrates that to the new DB2 installation where the instances and databases will be upgraded.
Cleanup Downloaded Files v2	This step removes files and archives that were downloaded to the target system during previous workflow steps.
Backup DB2 Server Configuration	This step backs up the existing DB2 setup environment and configuration before attempting to upgrade the instance and databases.
Prerequisites Checks for DB2 Instance and Database Upgrade	This step checks for the DB2 database upgrade eligibility.
Shutdown DB2 Instances	This step scans for all the running instances and active databases against the specified DB2 installation location and shuts them down.
Upgrade DB2 Instances	This step upgrades the DB2 instances.
Startup DB2 Instances	This step restarts DB2 instances.
Verify DB2 Upgrade Instances	This step verifies the DB2 instances post the upgrade from the existing DB2 installation to new DB2 installation.
Upgrade DB2 Databases v2	This step upgrades DB2 databases from the existing DB2 installation to new DB2 installation.
Verify DB2 Upgrade Databases	This step verifies the DB2 databases post the upgrade from the existing DB2 installation to new DB2 installation for the respective instances.
Cleanup Downloaded	This step removes files and archives that were downloaded to the target

Steps Used by DB2 - Upgrade Instance and Database , continued

Workflow Step	Description
Files v2	system during previous workflow steps.
Discover DB2 Databases	<p>This step audits the server's physical environment looking for DB2 databases.</p> <p>Note: Discovery is ONLY additive. It will not remove instances or databases currently in your environment. It is the end-user's responsibility to delete content that is no longer in use.</p> <p>In cluster situations where one node is active while other nodes are inactive, Discovery will only find instances and databases on the active node. Nothing will be added to inactive nodes.</p>

How to Run this Workflow

The following instructions show you how to customize and run the DB2 - Upgrade Instance and Database workflow in your environment.

Tip: For detailed instructions to run DMA workflows, see *DMA Quick Start Tutorial*.

The workflow provides default values for some parameters. These default values are usually sufficient for a "typical" installation. You can override the defaults by specifying parameter values in the deployment. You can also expose additional parameters in the workflow, if necessary, to accomplish more advanced scenarios. Any parameters not explicitly specified in the deployment will have the default values listed in ["Parameters for DB2 - Upgrade Instance and Database" on page 194](#).

Note: Before following this procedure, review the ["Prerequisites" on page 187](#), and ensure that all requirements are satisfied.

To use the DB2 - Upgrade Instance and Database workflow:

1. Create a deployable copy of the workflow (see "Create a Deployable Workflow" in *DMA Quick Start Tutorial*)

Determine the values that you will specify for the following parameters.

The following tables describe the required and optional input parameters for this workflow.

Parameters Defined in this Step: Gather Parameters for DB2 Upgrade Instance and Database

Parameter Name	Example Value	Description
DB2 Existing Installation Location	/opt/ibm/db2/v10.1	The fully-qualified absolute directory path where the current version of DB2 software is already installed and set up with instances and databases.
DB2 Installation Location	/opt/ibm/db2/v10.1_to_v10.5	The fully-qualified absolute directory path where the upgrade version of DB2 software will be installed to upgrade the instances and databases.
DB2 Software Binaries	v10.5_aix64_server_t.tar.gz	Name of the DB2 installer archive file. Obtained from IBM. If the file is not found in DB2 Archive Location (/tmp/dma/archive), It will be downloaded from the SA repository.

Parameters Defined in this Step: Gather Advanced Parameters for DB2 Upgrade Instance and Database

Parameter Name	Example Value	Description
Staging Directory	/tmp/software/staging	Fully-qualified path of the directory where the DB2 installer will be extracted from archive. Will be cleaned up at end of workflow execution. Default: If no input is provided /tmp/software/staging will be created.
Clean on Failure	Yes	Flag that determines whether to clean up on workflow failure. If set to 'yes', the workflow will clean up the downloaded files, installation location and the staging location. Valid values are 'Yes' and 'No'. The default value is 'Yes'.
Clean on Success	Yes	Flag that determines whether to clean up on workflow success. If set to 'yes', the workflow will clean up the downloaded files. The default value is 'Yes'.

Parameters Defined in this Step: Gather Advanced Parameters for DB2 Upgrade Instance and Database, continued

Parameter Name	Example Value	Description
DB2 Archive Location	/tmp/dma/archive	Location on the target machine where the DB2 binaries will be stored prior to the installation. The default value is /tmp/dma/archive.
DB2 Configuration Backup Location	/tmp/dma/config_bkp	Directory location where the DB2 Server, instance and database level configuration will be backed up in different files. The default value is set '/tmp/dma/config_bkp'.
DB2 Installation Type	TYPICAL	The type of DB2 installation supported by IBM. It can be either COMPACT, TYPICAL or CUSTOM. The default value is 'TYPICAL'. If set the CUSTOM, you should provide the DB2 installation responsefile with the custom parameter values.
DB2 Product Edition	DB2_SERVER_EDITION	The product that you want to install, for example, DB2 Workgroup Edition, DB2 Enterprise Edition only, or other editions. The default value is set to 'DB2_SERVER_EDITION' for DB2 10.5 in this step. If upgrading to DB2 version 9.7 or 10.1 then you should use 'ENTERPRISE_SERVER_EDITION'.
DB2 Product Installation Language	EN	The language(s) you want installed. If you do not enable any language keywords, then the English language (EN) will be installed by default. Please refer IBM install guide for the more details.
DB2 Product License	ACCEPT	Modify the value of the following LIC_AGREEMENT keyword to indicate that you have read and agreed to the license agreement file in the db2/license directory on the installation media. Default value is set to 'ACCEPT'
DB2 Staging Location	/tmp/software/staging	Location on the target machine where the DB2 software installation binaries will be extracted. The default value is /tmp/dma/staging.

Parameters Defined in this Step: Gather Advanced Parameters for DB2 Upgrade Instance and Database, continued

Parameter Name	Example Value	Description
DB2 Upgrade Check Logfile Location	/tmp	Directory location on target machine where the pre-upgrade check logfile will be created if it runs. The default location value is '/tmp'. The only valid values are /tmp or /var/tmp.
Install Tivoli System Automation Multiplatforms	NO	If set to "YES", IBM Tivoli System Automation for Multiplatforms (SA MP) is installed with required components. Do not specify any value if installing DB2 10.1 (or higher version) since this option is deprecated.
Trust SSL Certificates	True	If 'True', this step will trust any SSL used to connect to the DMA Web Service.
User Defined Responsefile		The user response file that will be used to provision DB2 Software. If the user response file is not specified, the workflow will use the deployment parameters and create a default response file using the default configuration set. If responsefile is provided, workflow will use the user specified responsefile parameter values.
Web Service Password	--	Password for the HPE DMA Discovery web service API to discover and update the metadata in DMA.
Web Service URL	--	URL for the HPE DMA Discovery web service API to discover and update metadata in DMA.
Web Service User	--	User for the HPE DMA Discovery web service API to discover and update metadata in DMA.

2. In the workflow editor, expose any additional parameters that you need. You will specify values for those parameters when you create the deployment or at runtime.
3. Save the changes to the workflow (click **Save** in the lower right corner).
4. Create a new deployment. See "Create a Deployment" in *DMA Quick Start Tutorial* for instructions.

5. On the Parameters tab, specify values (or set the type to Runtime Value) for the required parameters listed in step 2 and any additional parameters that you have exposed. You do not need to specify values for those parameters whose default values are appropriate for your environment.
6. On the Targets tab, specify one or more targets for this deployment.
7. Save the deployment (click **Save** in the lower right corner).
8. Run the workflow using this deployment, specifying any runtime parameters. See "Run Your Workflow" in *(DMA Quick Start Tutorial* for instructions.

To verify the results:

The workflow will complete and report SUCCESS on the Console if it has run successfully. If an error occurs during workflow execution, the error is logged, and the workflow terminates in the FAILURE state.

Parameters for DB2 - Upgrade Instance and Database

The following tables describe the required and optional input parameters for this workflow.

Parameters Defined in this Step: Gather Parameters for DB2 Upgrade Instance and Database

Parameter Name	Required	Example Value	Description
DB2 Existing Installation Location	required	/opt/ibm/db2/v10.1	The fully-qualified absolute directory path where the current version of DB2 software is already installed and set up with instances and databases.
DB2 Installation Location	required	/opt/ibm/db2/v10.1_to_v10.5	The fully-qualified absolute directory path where the upgrade version of DB2 software will be installed to upgrade the instances and databases.
DB2 Software Binaries	required	v10.5_aix64_server_t.tar.gz	Name of the DB2 installer archive file. Obtained from IBM. If the file is not found in DB2 Archive Location

Parameters Defined in this Step: Gather Parameters for DB2 Upgrade Instance and Database, continued

Parameter Name	Required	Example Value	Description
			(/tmp/dma/archive), It will be downloaded from the SA repository.

Parameters Defined in this Step: Gather Advanced Parameters for DB2 Upgrade Instance and Database

Parameter Name	Required	Example Value	Description
Staging Directory	optional	/tmp/software/staging	Fully-qualified path of the directory where the DB2 installer will be extracted from archive. Will be cleaned up at end of workflow execution. Default: If no input is provided /tmp/software/staging will be created.
Clean on Failure	optional	Yes	Flag that determines whether to clean up on workflow failure. If set to 'yes', the workflow will clean up the downloaded files, installation location and the staging location. Valid values are 'Yes' and 'No'. The default value is 'Yes'.
Clean on Success	optional	Yes	Flag that determines whether to clean up on workflow success. If set to 'yes', the workflow will clean up the downloaded files. The default value is 'Yes'.
DB2 Archive Location	optional	/tmp/dma/archive	Location on the target machine where the DB2 binaries will be stored prior to the installation. The default value is /tmp/dma/archive.
DB2 Configuration Backup Location	optional	/tmp/dma/config_bkp	Directory location

Parameters Defined in this Step: Gather Advanced Parameters for DB2 Upgrade Instance and Database, continued

Parameter Name	Required	Example Value	Description
			where the DB2 Server, instance and database level configuration will be backed up in different files. The default value is set <code>'/tmp/dma/config_bkp'</code> .
DB2 Installation Type	optional	TYPICAL	The type of DB2 installation supported by IBM. It can be either COMPACT, TYPICAL or CUSTOM. The default value is 'TYPICAL'. If set the CUSTOM, you should provide the DB2 installation responsefile with the custom parameter values.
DB2 Product Edition	optional	DB2_SERVER_EDITION	The product that you want to install, for example, DB2 Workgroup Edition, DB2 Enterprise Edition only, or other editions. The default value is set to 'DB2_SERVER_EDITION' for DB2 10.5 in this step. If upgrading to DB2 version 9.7 or 10.1 then you should use 'ENTERPRISE_SERVER_EDITION'.
DB2 Product Installation Language	optional	EN	The language(s) you want installed. If you do not enable any language keywords, then the English language (EN) will be installed by default. Please refer IBM install guide for the more details.
DB2 Product License	optional	ACCEPT	Modify the value of the following LIC_AGREEMENT

Parameters Defined in this Step: Gather Advanced Parameters for DB2 Upgrade Instance and Database, continued

Parameter Name	Required	Example Value	Description
			keyword to indicate that you have read and agreed to the license agreement file in the db2/license directory on the installation media. Default value is set to 'ACCEPT'
DB2 Staging Location	optional	/tmp/software/staging	Location on the target machine where the DB2 software installation binaries will be extracted. The default value is /tmp/dma/staging.
DB2 Upgrade Check Logfile Location	optional	/tmp	Directory location on target machine where the pre-upgrade check logfile will be created if it runs. The default location value is '/tmp'. The only valid values are /tmp or /var/tmp.
Install Tivoli System Automation Multiplatforms	optional	NO	If set to "YES", IBM Tivoli System Automation for Multiplatforms (SA MP) is installed with required components. Do not specify any value if installing DB2 10.1 (or higher version) since this option is deprecated.
Trust SSL Certificates	optional	True	If 'True', this step will trust any SSL used to connect to the DMA Web Service.
User Defined Responsefile	optional		The user response file that will be used to provision DB2 Software. If the user response file is not specified, the workflow will use the deployment parameters and create a default

Parameters Defined in this Step: Gather Advanced Parameters for DB2 Upgrade Instance and Database, continued

Parameter Name	Required	Example Value	Description
			response file using the default configuration set. If responsefile is provided, workflow will use the user specified responsefile parameter values.
Web Service Password	optional	--	Password for the HPE DMA Discovery web service API to discover and update the metadata in DMA.
Web Service URL	optional	--	URL for the HPE DMA Discovery web service API to discover and update metadata in DMA.
Web Service User	optional	--	User for the HPE DMA Discovery web service API to discover and update metadata in DMA.

MySQL

Workflow type	Workflow name
Provisioning	"MySQL - Install Instance" on page 240
	"MySQL - Create Database" on page 246
	"MySQL - Start or Stop" on page 252
	"MySQL Drop Database" on page 235
	MySQL - Upgrade Instance
Release Management	MySQL - SQL Release
Compliance	"MySQL - Compliance Audit" on the next page

MySQL - Compliance Audit

The MySQL - Compliance Audit workflow enables you to audit an instance of MySQL database for compliance with the following Center for Internet Security (CIS) benchmarks and, optionally, compare the audit results to the related Payment Card Industry (PCI) and Sarbanes-Oxley (SOX) requirements:

- CIS Security Benchmark for MySQL Enterprise Edition 5.6, June 2015
- Payment Card Industry Data Security Standard Version 3.1, April 2015
- Sarbanes-Oxley Act of 2002 Section 302

This workflow audits an instance of MySQL database using CIS Level 1 and Level 2 benchmarks. It will then compare the results to the pertinent PCI and SOX requirements, where applicable. The audit identifies compliance related problems with a MySQL instance.

To use this workflow in your environment, see the following information:

Topic	Information Included
"Prerequisites for this Workflow" on the next page	List of prerequisites that must be satisfied before you can run this workflow
"How this Workflow Works" on page 202	Information about what the workflow does, including validation checks performed, steps executed, and step descriptions
"How to Run this Workflow" on page 204	Instructions for running this workflow in your environment
"Sample Scenarios" on page 208	Examples of typical parameter values for this workflow
"Parameters for MySQL - Compliance Audit" on page 213	List of input parameters for this workflow

Prerequisites for this Workflow

Be sure that the following prerequisites are satisfied before you run the MySQL - Compliance Audit workflow:

- The latest DMA solution packs require the latest DMA platform. To use the latest solution packs, update the DMA platform. DMA10.50.001.000 solution packs are supported on DMA10.50.001.000 (and later).
- You have installed the Database Compliance solution pack.

The information presented here assumes the following: show assumptions

- DMA is installed and operational.
- At least one suitable target server (database) is available.
- You are logged in to the DMA web interface.
- You have permission to create, edit, and deploy copies of the workflows included in this solution pack.

For more information about prerequisites for MySQL database, refer to the [MySQL Server Documentation](#).

How this Workflow Works

This workflow performs the following actions:

- Prepares to run the workflow by gathering information about the target MySQL server instance and validating parameter values.
- Audits the various configuration settings specified in the pertinent CIS, SOX, or PCI benchmark.
- Composes and sends an email containing the results of the audit.

Note: The emails are sent through the mail server configured on the HPE DMA server. You can configure the mail server in the path below:

DMA setup > Configuration > Outgoing Mail > Server.

Validation Checks Performed

This workflow validates the following conditions:

1. Any Excluded Checks specified by the user refer to actual CIS, SOX, or PCI benchmark checks.
2. Any email addresses specified are valid addresses.
3. The workflow can create the temporary file that will store the compliance check results.

Steps Executed

The MySQL - Compliance Audit workflow includes the following steps. Each step must complete successfully before the next step can start. If a step fails, the workflow reports a failure and all subsequent steps are skipped.

Steps Used by Run MySQL Compliance Audit

Workflow Step	Description
MySQL - Gather Parameters for MySQL Compliance	This step gathers two pieces of information: (1) the type of compliance audit to perform and (2) the list of compliance checks to exclude from the audit.
MySQL - Gather Advanced Parameters for MySQL Compliance	This step gathers the optional parameters for MySQL compliance.
Validate Compliance Parameters v2	<p>This step validates the input parameters specified in the previous steps. It validates the list of excluded checks to ensure that all specified checks in the list correspond to actual Center for Internet Security (CIS) benchmark items. It also validates the email information to ensure that all specified email addresses are valid.</p> <p>The step then creates the path to the temporary file that will store the results of the current audit as the workflow is running. This file is deleted after the audit report is sent.</p>

Steps Used by Run MySQL Compliance Audit, continued

Workflow Step	Description
MySQL - Prepare MySQL Compliance Check	<p>This step determines whether workflow can perform the following actions on the target system:</p> <ul style="list-style-type: none"> • Check database connectivity • Check if MySQL configuration path is a valid file path. <p>If the workflow can perform these actions, it is capable of running the Center for Internet Security (CIS) Security Configuration Benchmark compliance tests.</p>
MySQL - Audit Operating System Level Configuration	This step audits the recommendations related to the operating system on which the MySQL database server is running.
MySQL - Audit File System Permissions	This step audits the file system permissions that are critical for keeping the data and configuration of the MySQL server secure.
MySQL - Audit General Settings	This step audits the recommendations related to various parts of the database server.
MySQL - Audit MySQL Permissions	This step audits the recommendations related to user privileges.
MySQL - Audit Auditing and Logging	This step audits the guidance with respect to MySQL's logging behavior.
MySQL - Audit Authentication	This step validates the configuration recommendations that pertain to the authentication mechanisms of MySQL.
MySQL - Audit Network	This step validates the recommendations related to how the MySQL server uses the network.
MySQL - Audit Replication	This step validates the recommendations related to replicating data from one server to another.
Validate Post Compliance Checks	<p>This step reads the temporary file that contains the results of the compliance audit and prints the audit results to the DMA Console. It also creates (or updates) the compliance metadata fields for the target.</p> <p>If email addresses were specified, it also creates a report in HTML format that will be emailed to those addresses by a later step in the workflow.</p>
Send Compliance Email v2	If email addresses are provided, this step sends the previously generated compliance audit report to the specified email addresses.
Delete File	This step deletes the specified file on the target server.

Note: For input parameter descriptions and defaults, see "[Parameters for MySQL - Compliance Audit](#)" on page 213.

How to Run this Workflow

The following instructions show you how to customize and run the MySQL - Compliance Audit workflow in your environment.

The workflow provides default values for some parameters. These default values are usually sufficient for a "typical" installation. You can override the defaults by specifying parameter values in the deployment. You can also expose additional parameters in the workflow, if necessary, to accomplish more advanced scenarios. Any parameters not explicitly specified in the deployment will have the default values listed in ["Parameters for MySQL - Compliance Audit" on page 213](#).

Note: Before following this procedure, review the ["Prerequisites for this Workflow" on page 201](#), and ensure that all requirements are satisfied.

To use the Run MS SQL Compliance Audit workflow:

1. Create a deployable copy of the workflow.
2. Determine the values that you will specify for the following parameters:

Parameters Defined in this Step: MySQL - Gather Parameters for MySQL Compliance

Parameter Name	Default Value	Required	Description
Compliance Type	CIS	optional	Type of compliance report that will be generated by the workflow. Supported types are: CIS = Center for Internet Security (CIS) Security Configuration Benchmark PCI = Payment Card Industry (PCI) Data Security Standard SOX = Sarbanes-Oxley (SOX) sections 302.2, 302.4b, 302.4c, and 302.5 requirements
Excluded Compliance Checks	no default	optional	Comma-separated list of compliance checks to exclude from the audit. For example: 1.2, 2, 3.*, 5*, 6.1.2 Note: Make sure that the checks specified here correspond with the compliance audit type (CIS, PCI, or SOX) that you are running.

Parameters Defined in this Step: MySQL - Gather Parameters for MySQL Compliance, continued

Parameter Name	Default Value	Required	Description
MySQL Configuration File	no default	optional	Absolute path of the my.cnf file for the given instance. For example: /usr/my.cnf, /etc/my.cnf
MySQL Password	no default	required	MySQL password for the given MySQL account.
MySQL User Name	no default	required	MySQL user account that has access to the 'mysql' and 'information_schema' databases.

Parameters Defined in this Step: MySQL - Gather Advanced Parameters for MySQL Compliance

Parameter Name	Default Value	Required	Description
Email Addresses to Receive Report	no default	required	Comma-separated list of email addresses for those individuals or groups who will receive a copy of the compliance audit report.
Latest MySQL Version Number	no default	required	Latest MySQL version number containing the latest security patch. For example: 5.6.25.

Note: This is the minimum set of parameters required to run this workflow. You may need to expose additional parameters depending on your objectives.

See ["Parameters for MySQL - Compliance Audit" on page 213](#) for detailed descriptions of all input parameters for this workflow, including default values.

3. In the workflow editor, expose any additional parameters that you need. You will specify values for those parameters when you create the deployment or at runtime.
4. Save the changes to the workflow (click **Save** in the lower right corner).
5. Create a new deployment.
6. On the Parameters tab, specify values (or set the type to Runtime Value) for the required

parameters listed in step 2 and any additional parameters that you have exposed. You do not need to specify values for those parameters whose default values are appropriate for your environment.

7. On the Targets tab, specify one or more targets for this deployment.
8. Save the deployment (click **Save** in the lower right corner).
9. Run the workflow using this deployment, specifying any runtime parameters.

To verify the results:

The workflow will complete and report SUCCESS on the Console if it has run successfully. If an error occurs during workflow execution, the error is logged, and the workflow terminates in the FAILURE state.

Information about each compliance check is displayed in the step output on the Console (and the History page) for each of the audit steps.

A summary of the compliance audit is also displayed in the step output for the Validate Post Compliance Checks step.

To view the reports:

A compliance audit summary in HTML format is emailed to all parties on the Email Addresses to Receive Report list.

After you run this workflow, you can generate two types of compliance reports on the Reports page:

- Database Compliance Report
- Database Compliance Detail Report

To access the Database Compliance reports:

1. Go to the Reports page.
2. At the bottom of the page, specify the following settings:

For the Database Compliance Report:

- a. Select the Database Compliance report.
- b. Select the organization where your target resides.
- c. Because this report lists the latest compliance audit reports for all targets in the specified organization, you do not specify a Server, Database, or Time span.

For the Database Compliance Detail Report:

- a. Select the Database Compliance Details report.
- b. Select the organization where your target resides.
- c. Specify the Server and Instance that you selected when you created your deployment.

3. Click **Run report**.

Sample Scenarios

This topic shows you how to use various parameters to achieve the following compliance audit scenarios in your environment using the MySQL - Compliance Audit workflow.

Scenario 1: Perform a Partial CIS Compliance Audit and Email the Results

In the scenario, the following checks are excluded from the audit:

- Section 7: Replication
- Section 9: Surface Area Configuration Tool

A summary report is sent to the three parties listed in the Email Addresses to Receive Report parameter.

Parameter Name	Example Value	Description
Compliance Type	CIS	<p>Type of compliance report that will be generated by the workflow. Supported types are:</p> <p>CIS = Center for Internet Security (CIS) Security Configuration Benchmark</p> <p>PCI = Payment Card Industry (PCI) Data Security Standard</p> <p>SOX = Sarbanes-Oxley (SOX) sections 302.2, 302.4b, 302.4c, and 302.5 requirements</p>
Excluded Compliance Checks	7.*,9.*	<p>Comma-separated list of compliance checks to exclude from the audit. For example:</p> <p>1.2, 2, 3.*, 5*, 6.1.2</p> <p>Note: Make sure that the checks specified here correspond with the compliance audit type (CIS, PCI, or SOX) that you are running.</p>
Email Addresses to Receive Report	MySQLDBAdminTeam@mycompany.com, MySQLDBAdminMgr@mycompany.com, CustomerSupportTeam@mycompany.com	Comma-separated list of email addresses for those individuals or groups who

Parameter Name	Example Value	Description
		will receive a copy of the compliance audit report.

Note: Some of these parameters are not exposed by default in the deployment.

Be sure that the default values for all remaining input parameters are appropriate for your environment.

Scenario 2: Perform a Full PCI Compliance Audit and Email the Results

A summary report is sent to the three parties listed in the Email Addresses to Receive Report parameter.

Parameter Name	Example Value	Description
Compliance Type	PCI	<p>Type of compliance report that will be generated by the workflow. Supported types are:</p> <p>CIS = Center for Internet Security (CIS) Security Configuration Benchmark</p> <p>PCI = Payment Card Industry (PCI) Data Security Standard</p> <p>SOX = Sarbanes-Oxley (SOX) sections 302.2, 302.4b, 302.4c, and 302.5 requirements</p>
Email Addresses to Receive Report	MySQLDBAdminTeam@mycompany.com, MySQLDBAdminMgr@mycompany.com, CustomerSupportTeam@mycompany.com	Comma-separated list of email addresses for those individuals or groups who will receive a copy of the compliance audit report.

Note: Some of these parameters are not exposed by default in the deployment.

Be sure that the default values for all remaining input parameters are appropriate for your environment.

Scenario 3: Perform a Full SOX Compliance Audit, Email the Results, and Configure Windows Domain User Using Runtime Parameters

A summary report is sent to the three parties listed in the Email Addresses to Receive Report parameter.

Note: By using a runtime parameter for the password, you can ensure that the password used is always the latest.

To specify the password at the time you execute a deployment with runtime parameters, perform the following additional steps:

1. When you make a copy of the workflow, expand the appropriate step, and then set the MySQL Instance Account and MySQL Password to
- User selected -.
2. When you create a deployment from the copy of the workflow, set the parameter types to **Runtime Value**.
3. When you execute the deployment, specify the MySQL Instance User and MySQL Password.

Parameter Name	Example Value	Description
Compliance Type	SOX	Type of compliance report that will be generated by the workflow. Supported types are: CIS = Center for Internet Security (CIS) Security Configuration Benchmark PCI = Payment Card Industry (PCI) Data Security Standard SOX = Sarbanes-Oxley (SOX) sections 302.2, 302.4b, 302.4c, and 302.5 requirements
Email Addresses to Receive Report	MySQLDBAdminTeam@mycompany.com, MySQLDBAdminMgr@mycompany.com, CustomerSupportTeam@mycompany.com	Comma-separated list of email addresses for those individuals or groups who will receive a copy of the compliance audit report.
Latest MySQL Version Number	5.6.25	The latest build of MySQL. Example value would be "5.6.25". If no value is given, the related

Parameter Name	Example Value	Description
		Compliance check will be skipped.

Note: Some of these parameters are not exposed by default in the deployment.

Be sure that the default values for all remaining input parameters are appropriate for your environment.

Scenario 4: Perform a Full CIS Compliance Audit and Display the Results on the DMA Console

In the scenario, all scorable checks are performed, and the compliance audit report is displayed only on the DMA Console. In this case, a summary report is not emailed. This scenario would be appropriate for initial testing.

It is not necessary to specify any input parameters in this scenario unless the MySQL inventory file is located in a non-standard directory.

Parameter Name	Example Value	Description
Compliance Type	CIS	Type of compliance report that will be generated by the workflow. Supported types are: CIS = Center for Internet Security (CIS) Security Configuration Benchmark PCI = Payment Card Industry (PCI) Data Security Standard SOX = Sarbanes-Oxley (SOX) sections 302.2, 302.4b, 302.4c, and 302.5 requirements

Be sure that the default values for all remaining input parameters are appropriate for your environment.

Parameters for MySQL - Compliance Audit

The following tables describe the required and optional input parameters for this workflow. Some of these parameters are not initially visible in a deployment. For most parameters, if you do not specify a value for a parameter, a default value is assigned.

Only those parameters that are configurable in a standard deployment are listed here. Input parameters that must be mapped to output parameters of previous steps are not listed.

Parameters Defined in this Step: Gather Parameters for MySQL Compliance

Parameter Name	Default Value	Required	Description
Compliance Type	CIS	optional	Type of compliance report that will be generated by the workflow. Supported types are: <ul style="list-style-type: none"> CIS = Center for Internet Security (CIS) Security Configuration Benchmark PCI = Payment Card Industry (PCI) Data Security Standard SOX = Sarbanes-Oxley (SOX) sections 302.2, 302.4b, 302.4c, and 302.5 requirements
Excluded Compliance Checks	no default	optional	Comma-separated list of compliance checks to exclude from the audit. For example: 1.2, 2, 3.*, 5*, 6.1.2 Note: Make sure that the checks specified here correspond with the compliance audit type (CIS, PCI, or SOX) that you are running.
MySQL Configuration File	no default	optional	Absolute path of the my.cnf file for the given instance. For example: /usr/my.cnf, /etc/my.cnf
MySQL Password	no default	optional	MySQL password for the given MySQL account.
MySQL User Name	no default	optional	MySQL user account that has access to the 'mysql' and 'information_schema' databases.

Parameters Defined in this Step: Gather Advanced Parameters for MySQL Compliance

Parameter Name	Default Value	Required	Description
Email Addresses to Receive Report	no default	optional	Comma-separated list of email addresses for those individuals or groups who will receive a copy of the compliance audit report.
Latest MySQL Version Number	no default	optional	Latest MySQL version number containing the latest security patch. For example: 5.6.25.

MySQL - SQL Release

The MySQL - SQL Release workflow enables you to executes the given MySQL scripts on the target database. The given scripts are executed one by one. When any one of the script fails, the workflow exits with failure status.

To use this workflow in your environment, see the following information:

Topic	Information Included
"Prerequisites for this Workflow"	List of prerequisites that must be satisfied before you can run this workflow
"How this Workflow Works"	Information about what the workflow does, including validation checks performed, steps executed, and step descriptions
" How to Run this Workflow"	Instructions for running this workflow in your environment
"Parameters for MySQL - SQL Release"	List of input parameters for this workflow

Prerequisites for this Workflow

Be sure that the following prerequisites are satisfied before you run the MySQL - Upgrade Instance workflow:

- This solution requires DMA version 10.40 (or later).
- You have installed the Database Release Management solution pack.

The workflow must be able to:

- Log in to the MySQL instance using MySQL login credentials.
- The MySQL login credentials used in the workflow needs to have necessary permissions to perform the operations specified in the SQL scripts.

For more information about prerequisites for MySQL database, refer to the [MySQL Server Documentation](#).

How this Workflow Works

This workflow performs the following actions:

Executes the given MySQL scripts on the target database.

Steps Executed by the Workflow

The MySQL - SQL Release workflow includes the following steps. Each step must complete successfully before the next step can start. If a step fails, the workflow reports a failure and all subsequent steps are skipped.

Steps executed by MySQL - SQL Release workflow

Workflow Step	Description
MySQL - Gather Parameters for SQL Release	This step gathers the parameters required to execute the MySQL – SQL Release workflow.
MySQL - Validate Parameters for SQL Release	This step validates the input parameters to MySQL – SQL Release workflow.
MySQL - Check Prohibited Grant Privileges	This step checks for existence of prohibited grant privileges in the script files.
Download Software	This step automates the transfer of files from the HP SA Software Library to individual managed servers for use in downstream workflow steps. Verifies checksum of each file transferred.
MySQL - Check Prohibited Database Commands	This step checks for existence of prohibited database commands in the script file.
Cleanup Downloaded Files	This step removes all the downloaded files and archives.
MySQL - Check Prohibited Regular Expression	This step checks for existence of prohibited regular expression in the script file.
MySQL - Check MySQL Syntax	This step checks for syntax errors in the script files. It displays the total count of errors in all the script files.
MySQL - Execute Scripts	This step executes the MySQL scripts on the target database.
MySQL - Execute Rollback Scripts	This step executes the rollback scripts on the target database.

Note: For input parameter descriptions and defaults, see "[Parameters for MySQL - SQL Release](#)" on page 220.

How to Run this Workflow

The following instructions show you how to customize and run the MySQL - SQL Release workflow in your environment.

Tip: For detailed instructions to run DMA workflows, see *DMA Quick Start Tutorial*.

The workflow provides default values for some parameters. These default values are usually sufficient for a "typical" installation. You can override the defaults by specifying parameter values in the deployment. You can also expose additional parameters in the workflow, if necessary, to accomplish more advanced scenarios. Any parameters not explicitly specified in the deployment will have the default values listed in ["Parameters for MySQL - SQL Release" on page 220](#).

Note: Before following this procedure, review the ["Prerequisites for this Workflow" on page 215](#), and ensure that all requirements are satisfied.

To use the Run MySQL - SQL Release workflow:

1. Create a deployable copy of the workflow (see "Create a Deployable Workflow" in *DMA Quick Start Tutorial*)
2. Determine the values that you will specify for the following parameters.

Parameters Defined in this Step: MySQL - Gather Parameters for SQL Release

Parameter Name	Default Value	Required	Description
Check MySQL Syntax Run Flag	Y	Required	Boolean parameter to specify whether syntax check needs to be executed on the MySQL Scripts and on the Rollback Scripts. Default Value is Y.
Check Prohibited Grant Privileges Run Flag	Y	Required	Boolean parameter to specify whether the MySQL Script file needs to be checked for prohibited grant privilege commands. Default Value is Y.
Check Prohibited MySQL Commands Run Flag	Y	Required	Boolean parameter to specify whether the MySQL Script file needs to be checked for prohibited MySQL commands.
Check Prohibited Regular Expression Run Flag	Y	Required	Boolean parameter to specify whether the MySQL Script file needs to be checked for user specified regular expression.

Parameters Defined in this Step: MySQL - Gather Parameters for SQL Release, continued

Parameter Name	Default Value	Required	Description
Database Password	no default	Required	Password to connect to the database.
Database User Name	no default	Required	User Account to connect to the database.
Display MySQL Script Output		Required	Boolean parameter to specify whether the output of MySQL Script file is to be displayed on DMA console.
Display SQL Length	200	Required	Integer specifying the length of the MySQL script file to be displayed on DMA console in case of exception.
Execute Rollback on Failure	N	Required	Boolean parameter to specify whether rollback script is to be executed on failure of execution of MySQL script files.
MySQL Script List	no default	Required	Comma separated list of script files to be executed on the target database.
Prohibited Grant Privileges	grant all, grant insert, grant create user, grant delete, grant select , grant create routine, grant execute on	Required	Comma separated list of prohibited grant privilege commands.
Prohibited MySQL Commands	create database, drop database, create user, drop user	Required	Comma separated list of prohibited MySQL commands.
Prohibited Regular Expression	no default	Required	Regular pattern that should not exist in the MySQL Script file.
Rollback Script List	no default	Required	Comma separated list of rollback scripts to be executed on failure of execution of MySQL scripts.
Staging Directory	/tmp/mysql_sql_release	Required	Directory to place the Scripts downloaded from SA core.

3. In the workflow editor, expose any additional parameters that you need. You will specify values for those parameters when you create the deployment or at runtime.
4. Save the changes to the workflow (click **Save** in the lower right corner).

5. Create a new deployment. See "Create a Deployment" in *DMA Quick Start Tutorial* for instructions.
6. On the Parameters tab, specify values (or set the type to Runtime Value) for the required parameters listed in step 2 and any additional parameters that you have exposed. You do not need to specify values for those parameters whose default values are appropriate for your environment.
7. On the Targets tab, specify one or more targets for this deployment.
8. Save the deployment (click **Save** in the lower right corner).
9. Run the workflow using this deployment, specifying any runtime parameters. See "Run Your Workflow" in *(DMA Quick Start Tutorial* for instructions.

To verify the results:

The workflow will complete and report SUCCESS on the Console if it has run successfully. If an error occurs during workflow execution, the error is logged, and the workflow terminates in the FAILURE state.

Parameters for MySQL - SQL Release

The following tables describe the required and optional input parameters for this workflow.

Parameters Defined in this Step: MySQL - Gather Parameters for SQL Release

Parameter Name	Default Value	Required	Description
Check MySQL Syntax Run Flag	Y	required	If yes (Y), specifies whether syntax check needs to be executed on the MySQL Scripts and on the Rollback Scripts.
Check Prohibited Grant Privileges Run Flag	Y	required	If yes (Y), specifies whether the MySQL Script file needs to be checked for prohibited grant privilege commands.
Check Prohibited MySQL Commands Run Flag	Y	required	If yes (Y), specifies whether the MySQL Script file needs to be checked for prohibited MySQL commands.
Check Prohibited Regular Expression Run Flag	Y	required	If yes (Y), specifies whether the MySQL Script file needs to be checked for user specified regular expression.
Database Password	no default	required	Password to connect to the database.
Database User Name	no default	required	User Account to connect to the database. Example: root
Display MySQL Script Output	Y	required	If yes (Y), specifies whether the output of MySQL Script file is to be displayed on DMA console.
Display SQL Length	250	required	Specifies the length of the MySQL script file as an integer value to be displayed on DMA console in case of exception.
Execute Rollback on Failure	Y	required	If yes (Y), specifies whether rollback script is to be executed on failure of execution of MySQL script files.
MySQL Script List	ProperScript.sql	required	Specifies a comma separated list of script files to be executed on the target database.
Prohibited Grant Privileges	grant all, grant insert, grant create user, grant delete, grant select , grant create routine, grant execute on	required	Specifies a comma separated list of prohibited grant privilege commands.
Prohibited MySQL	create user, drop user	required	Specifies a comma separated list of prohibited MySQL commands.

Parameters Defined in this Step: MySQL - Gather Parameters for SQL Release, continued

Parameter Name	Default Value	Required	Description
Commands			
Prohibited Regular Expression		required	Specifies a regular pattern that should not exist in the MySQL Script file.
Rollback Script List	Rollbackscript.sql	required	Specifies a comma separated list of rollback scripts to be executed on failure of execution of MySQL scripts.
Staging Directory	/tmp/mysql_sql_release_hello	required	Specifies a directory to place the scripts downloaded from SA core.

MySQL - Upgrade Instance

This workflow upgrades the MySQL instance. The existing instance is taken as a backup and is stored in the location specified by the user. In-place RPM upgrade is performed if the upgrades are minor. The existing version is removed and a new installation is done for any major upgrades. After the RPM upgrade, upgrading the databases and the table is performed by running the `mysql_upgrade` utility.

To use this workflow in your environment, see the following information:

Topic	Information Included
"Prerequisites for this Workflow"	List of prerequisites that must be satisfied before you can run this workflow
"How this Workflow Works"	Information about what the workflow does, including validation checks performed, steps executed, and step descriptions
"How to Run this Workflow"	Instructions for running this workflow in your environment
"Parameters for MySQL - Upgrade Instance"	List of input parameters for this workflow

Prerequisites for this Workflow

Be sure that the following prerequisites are satisfied before you run the MySQL - Upgrade Instance workflow:

- This solution requires DMA version 10.40 (or later).
- You have installed the Database Release Management solution pack.
- If the MySQL client is not installed on the server, include the MySQL client in list of RPMs to be installed.

The workflow must be able to:

- Take dump of the existing databases.
- Upgrade the MySQL RPMs.
- Run the `mysql_upgrade` utility on all the databases.

For more information about prerequisites for MySQL database, refer to the [MySQL Server Documentation](#).

How this Workflow Works

This workflow performs the following actions:

Steps Executed by the Workflow

The MySQL - Upgrade Instance workflow includes the following steps. Each step must complete successfully before the next step can start. If a step fails, the workflow reports a failure and all subsequent steps are skipped.

Steps executed by MySQL - Upgrade Instance workflow

Workflow Step	Description
MySQL - Gather Parameters for MySQL Upgrade Instance	This step gathers parameters for MySQL Upgrade.
MySQL - Gather Advanced Parameters for MySQL Upgrade Instance	This step gathers advanced parameters for MySQL Upgrade. This step has few selected parameters that can be passed as an option to 'mysql_upgrade' command.
MySQL - Gather Advanced Parameters for Backup Dump	This step gathers advanced parameters for MySQL Dump. This step has few selected parameters that can be passed as an option to 'mysqldump' command.
MySQL - Validate Parameters for Download File	This step consolidates the list of files required to execute the MySQL - Upgrade Instance workflow.
Download Software	This step automates the transfer of files from the HP SA Software Library to individual managed servers for use in downstream workflow steps.
MySQL - Validate Upgrade	This step validates the pre-requisites for upgrading MySQL instance. For example, whether a direct upgrade from the existing version to the required version is possible or whether the dump file and the software binaries need to be deleted after the execution of the workflow.
Cleanup Downloaded Files	This step removes all downloaded files and archives.
MySQL - Validate Upgrade and Dump Parameters	This step validates the parameters passed as input for the mysqldump and mysql_upgrade utilities and consolidates all the input parameters in a single string.
MySQL - Backup Database	This step takes a dump of the MySQL databases for backup purpose.
MySQL - Start or Stop	This step starts or stops the MySQL service based on the action specified as input.
Cleanup Downloaded Files	This step removes all downloaded files and archives.
MySQL - Upgrade	This step does an in-place rpm upgrade or fresh installation of RPM.

Steps executed by MySQL - Upgrade Instance workflow, continued

Workflow Step	Description
Installation	
MySQL - Clean Dump File	This step removes the MySQL dump file from the system.
MySQL - Upgrade Database and Tables	This step runs the 'mysql_upgrade' utility on the upgraded MySQL instance.
MySQL - Verify Upgrade	This step verifies the version of the installed MySQL with the version that was to be installed.
Discover MySQL Databases	This step discovers the MySQL instances and databases on the target machine.

Note: For input parameter descriptions and defaults, see ["Parameters for MySQL - Upgrade Instance" on page 231](#).

How to Run this Workflow

The following instructions show you how to customize and run the MySQL - Upgrade Instance workflow in your environment.

Tip: For detailed instructions to run DMA workflows, see *DMA Quick Start Tutorial*.

The workflow provides default values for some parameters. These default values are usually sufficient for a "typical" installation. You can override the defaults by specifying parameter values in the deployment. You can also expose additional parameters in the workflow, if necessary, to accomplish more advanced scenarios. Any parameters not explicitly specified in the deployment will have the default values listed in ["Parameters for MySQL - Upgrade Instance" on page 231](#).

Note: Before following this procedure, review the ["Prerequisites for this Workflow" on page 223](#), and ensure that all requirements are satisfied.

To use the Run MySQL - Upgrade Instance workflow:

1. Create a deployable copy of the workflow (see "Create a Deployable Workflow" in *DMA Quick Start Tutorial*)
2. Determine the values that you will specify for the following parameters.

Parameters Defined in this Step: MySQL - Gather Parameters for MySQL Instance Upgrade

Parameter Name	Default Value	Required	Description
MySQL Backup Dump Location	/tmp	required	Specifies the location to store the dump of databases for backup purpose.
Software Binaries	no default	optional	Specifies a comma separated list of RPMs which needs to be installed.

Parameters Defined in this Step: MySQL - Gather Advanced Parameters for MySQL Instance Upgrade

Parameter Name	Default Value	Required	Description
Clean Dump File on Failure	False	optional	Specify if the dump file created as backup needs to be deleted on failure of the workflow
Clean Dump File	False	optional	Specify if the dump file created as backup needs to be deleted on successful execution of the workflow.

Parameters Defined in this Step: MySQL - Gather Advanced Parameters for MySQL Instance Upgrade, continued

Parameter Name	Default Value	Required	Description
on Success			
Clean Software Binaries on Failure	False	optional	Specify if the software binaries or configuration files downloaded from SA core needs to be deleted on failure of the workflow.
Clean Software Binaries on Success	False	optional	Specify if the software binaries or configuration files downloaded from SA core needs to be deleted on successful execution of the workflow.
MySQL Force Upgrade	True	optional	Force execution of mysql_upgrade utility, even if it has already been executed for current version of MySQL.
MySQL Upgrade Additional Options	no default	optional	Pipe delimited additional options that can be passed as input to mysql_upgrade utility. Example: --fields-enclosed-by , --no-autocommit True.
MySQL Upgrade Debug Info	no default	optional	Print debugging information, memory, and CPU statistics when program exits.
MySQL Upgrade Debug Log	no default	optional	Write debugging log to the given file. Example: d:t:o,/tmp/MySQL_Sample.log.
MySQL Upgrade Defaults Extra File	no default	optional	Read named option file in addition to usual option files.
MySQL Upgrade Defaults File	no default	optional	Read only named option file.
MySQL Upgrade Host	no default	optional	Machine Name or IP Address on which the MySQL server is to be upgraded.
MySQL Upgrade Parameter File	no default	optional	File containing additional parameters that needs to be passed as input to mysql_upgrade utility.
MySQL Upgrade Password	no default	optional	Password of the MySQL User account that can access the MySQL server that needs to be upgraded

Parameters Defined in this Step: MySQL - Gather Advanced Parameters for MySQL Instance Upgrade, continued

Parameter Name	Default Value	Required	Description
MySQL Upgrade Port	no default	optional	Port on which the MySQL service that needs to be upgraded is running.
MySQL Upgrade User	no default	optional	User Account of the MySQL server that needs to be upgraded.
MySQL Upgrade Verbose	no default	optional	Run mysql_upgrade utility in verbose mode.
MySQL Upgrade Write Bin Log	no default	optional	Write all statements from mysql_upgrade utility to binary log.
Staging Directory	no default	optional	Directory where the software binaries or configuration files available.

Parameters Defined in this Step: MySQL - Gather Advanced Parameters for Backup Dump

Parameter Name	Default Value	Required	Description
MySQL Dump Additional Options	no default	optional	Pipe delimited additional options for mysqldump. Example: --defaults-group-suffix abc --ignore-table ABC.SampleTable.
MySQL Dump All Database	True	optional	Dump all tables in all databases.
MySQL Dump Compatible Output	no default	optional	Produce output that is more compatible with other database systems or with older MySQL servers.
MySQL Dump Date	True	optional	Include dump date as "Dump completed on" comment if --comments is given.
MySQL Dump Debug Info	no default	optional	Print debugging information, memory, and CPU statistics when program exits.
MySQL Dump Debug Log	no default	optional	Write debugging log to the given file. Example : d:t:o,/tmp/MySQL_Sample.log.
MySQL	no	optional	Read named option file in addition to usual option files.

Parameters Defined in this Step: MySQL - Gather Advanced Parameters for Backup Dump, continued

Parameter Name	Default Value	Required	Description
Dump Defaults Extra File	default		
MySQL Dump Defaults File	no default	optional	Read only named option file.
MySQL Dump Events	True	optional	Dump events from dumped databases.
MySQL Dump Flush logs	no default	optional	Flush MySQL server log files before starting dump.
MySQL Dump Flush Privileges	no default	optional	Emit a FLUSH PRIVILEGES statement after dumping MySQL database.
MySQL Dump Host	no default	optional	Machine Name or IP Address of the MySQL Server.
MySQL Dump Lock All Tables	True	optional	Lock all tables across all databases.
MySQL Dump Log Error	no default	optional	Append warnings and errors to named file.
MySQL Dump Parameter File	no default	optional	File containing additional parameters that needs to be passed as input to mysqldump command.
MySQL Dump Password	no default	optional	Password for MySQL User.
MySQL Dump Result File	no default	optional	Name of the file to store the results of the mysqldump command.
MySQL Dump Routines	True	optional	Dump stored routines (procedures and functions) from dumped databases.
MySQL Dump User	no default	optional	MySQL User Account.

Parameters Defined in this Step: MySQL - Gather Advanced Parameters for Backup Dump, continued

Parameter Name	Default Value	Required	Description
MySQL Dump Verbose	no default	optional	Run the mysqldump command in verbose mode.

3. In the workflow editor, expose any additional parameters that you need. You will specify values for those parameters when you create the deployment or at runtime.
4. Save the changes to the workflow (click **Save** in the lower right corner).
5. Create a new deployment. See "Create a Deployment" in *DMA Quick Start Tutorial* for instructions.
6. On the Parameters tab, specify values (or set the type to Runtime Value) for the required parameters listed in step 2 and any additional parameters that you have exposed. You do not need to specify values for those parameters whose default values are appropriate for your environment.
7. On the Targets tab, specify one or more targets for this deployment.
8. Save the deployment (click **Save** in the lower right corner).
9. Run the workflow using this deployment, specifying any runtime parameters. See "Run Your Workflow" in *(DMA Quick Start Tutorial* for instructions.

To verify the results:

The workflow will complete and report SUCCESS on the Console if it has run successfully. If an error occurs during workflow execution, the error is logged, and the workflow terminates in the FAILURE state.

Parameters for MySQL - Upgrade Instance

The following tables describe the required and optional input parameters for this workflow.

Parameters Defined in this Step: MySQL - Gather Parameters for MySQL Upgrade Instance

Parameter Name	Default Value	Required	Description
MySQL Backup Dump Location	/tmp	required	Specifies the location to store the dump of databases for backup purpose.
Software Binaries	no default	optional	Specifies a comma separated list of RPMs which needs to be installed.

Parameters Defined in this Step: MySQL - Gather Advanced Parameters for MySQL Upgrade Instance

Parameter Name	Default Value	Required	Description
Clean Dump File on Failure	False	optional	Specify if the dump file created as backup needs to be deleted on failure of the workflow
Clean Dump File on Success	False	optional	Specify if the dump file created as backup needs to be deleted on successful execution of the workflow.
Clean Software Binaries on Failure	False	optional	Specify if the software binaries or configuration files downloaded from SA core needs to be deleted on failure of the workflow.
Clean Software Binaries on Success	False	optional	Specify if the software binaries or configuration files downloaded from SA core needs to be deleted on successful execution of the workflow.
MySQL Force Upgrade	True	optional	Force execution of mysql_upgrade utility, even if it has already been executed for current version of MySQL.
MySQL Upgrade Additional Options	no default	optional	Pipe delimited additional options that can be passed as input to mysql_upgrade utility. Example: --fields-enclosed-by , --no-autocommit True.
MySQL Upgrade Debug Info	no default	optional	Print debugging information, memory, and CPU statistics when program exits.

Parameters Defined in this Step: MySQL - Gather Advanced Parameters for MySQL Upgrade Instance, continued

Parameter Name	Default Value	Required	Description
MySQL Upgrade Debug Log	no default	optional	Write debugging log to the given file. Example: d:t:o,/tmp/MySQL_Sample.log.
MySQL Upgrade Defaults Extra File	no default	optional	Read named option file in addition to usual option files.
MySQL Upgrade Defaults File	no default	optional	Read only named option file.
MySQL Upgrade Host	no default	optional	Machine Name or IP Address on which the MySQL server is to be upgraded.
MySQL Upgrade Parameter File	no default	optional	File containing additional parameters that needs to be passed as input to mysql_upgrade utility.
MySQL Upgrade Password	no default	optional	Password of the MySQL User account that can access the MySQL server that needs to be upgraded
MySQL Upgrade Port	no default	optional	Port on which the MySQL service that needs to be upgraded is running.
MySQL Upgrade User	no default	optional	User Account of the MySQL server that needs to be upgraded.
MySQL Upgrade Verbose	no default	optional	Run mysql_upgrade utility in verbose mode.
MySQL Upgrade Write Bin Log	no default	optional	Write all statements from mysql_upgrade utility to binary log.
Staging Directory	no default	optional	Directory where the software binaries or configuration files available.

Parameters Defined in this Step: MySQL - Gather Advanced Parameters for Backup Dump

Parameter Name	Default Value	Required	Description
MySQL Dump	no default	optional	Pipe delimited additional options for mysqldump. Example: --defaults-group-suffix abc --ignore-table ABC.SampleTable.

Parameters Defined in this Step: MySQL - Gather Advanced Parameters for Backup Dump, continued

Parameter Name	Default Value	Required	Description
Additional Options			
MySQL Dump All Database	True	optional	Dump all tables in all databases.
MySQL Dump Compatible Output	no default	optional	Produce output that is more compatible with other database systems or with older MySQL servers.
MySQL Dump Date	True	optional	Include dump date as "Dump completed on" comment if --comments is given.
MySQL Dump Debug Info	no default	optional	Print debugging information, memory, and CPU statistics when program exits.
MySQL Dump Debug Log	no default	optional	Write debugging log to the given file. Example : d:t:o,/tmp/MySQL_Sample.log.
MySQL Dump Defaults Extra File	no default	optional	Read named option file in addition to usual option files.
MySQL Dump Defaults File	no default	optional	Read only named option file.
MySQL Dump Events	True	optional	Dump events from dumped databases.
MySQL Dump Flush logs	no default	optional	Flush MySQL server log files before starting dump.
MySQL Dump Flush Privileges	no default	optional	Emit a FLUSH PRIVILEGES statement after dumping MySQL database.
MySQL Dump Host	no default	optional	Machine Name or IP Address of the MySQL Server.
MySQL Dump Lock All Tables	True	optional	Lock all tables across all databases.
MySQL Dump Log Error	no default	optional	Append warnings and errors to named file.

Parameters Defined in this Step: MySQL - Gather Advanced Parameters for Backup Dump, continued

Parameter Name	Default Value	Required	Description
MySQL Dump Parameter File	no default	optional	File containing additional parameters that needs to be passed as input to mysqldump command.
MySQL Dump Password	no default	optional	Password for MySQL User.
MySQL Dump Result File	no default	optional	Name of the file to store the results of the mysqldump command.
MySQL Dump Routines	True	optional	Dump stored routines (procedures and functions) from dumped databases.
MySQL Dump User	no default	optional	MySQL User Account.
MySQL Dump Verbose	no default	optional	Run the mysqldump command in verbose mode.

MySQL Drop Database

The MySQL Drop Database workflow enables you to remove the target database from the MySQL instance and from the DMA environment.

To use this workflow in your environment, see the following information:

Topic	Information Included
"Prerequisites for this Workflow" on the next page	List of prerequisites that must be satisfied before you can run this workflow
"How this Workflow Works" on page 237	Information about what the workflow does, including validation checks performed, steps executed, and step descriptions
" How to Run this Workflow" on page 238	Instructions for running this workflow in your environment
"Parameters for MySQL - Drop Database" on page 239	List of input parameters for this workflow

Prerequisites for this Workflow

Be sure that the following prerequisites are satisfied before you run the MySQL Drop Database workflow:

- This solution requires DMA version 10.50.001.000 (or later).

The latest DMA solution packs require the latest DMA platform. To use the latest solution packs, update the DMA platform. DMA10.50.001.000 solution packs are supported on DMA10.50.001.000 (and later).

- You have installed the Database Provisioning solution pack.

The workflow must be able to:

- Log in to the MySQL instance using MySQL login credentials.
- Drop the database upon connecting to the MySQL instance.

The information presented here assumes the following: show assumptions

- DMA is installed and operational.
- At least one suitable target server (database) is available.
- You are logged in to the DMA web interface.
- You have permission to create, edit, and deploy copies of the workflows included in this solution pack.

For more information about prerequisites for MySQL database, refer to the [MySQL Server Documentation](#).

How this Workflow Works

This workflow performs the following actions:

- Drops a MySQL database and removes it from the DMA environment.

Steps Executed by the Workflow

The MySQL Drop Database workflow includes the following steps. Each step must complete successfully before the next step can start. If a step fails, the workflow reports a failure and all subsequent steps are skipped.

Steps Used by MySQL Drop Database

Workflow Step	Description
Gather Advanced Parameters for MySQL	This step gathers parameters to drop a MySQL database.
MySQL - Drop Database	This steps drops the database from the target machine.
Remove Database from Environment V2	This step removes the database from the DMA environment.

How to Run this Workflow

The following instructions show you how to customize and run the MySQL Drop Database workflow in your environment.

The workflow provides default values for some parameters. These default values are usually sufficient for a "typical" installation. You can override the defaults by specifying parameter values in the deployment. You can also expose additional parameters in the workflow, if necessary, to accomplish more advanced scenarios. Any parameters not explicitly specified in the deployment will have the default values listed in ["Parameters for MySQL - Drop Database" on the next page](#).

Note: Before following this procedure, review the ["Prerequisites for this Workflow" on page 236](#), and ensure that all requirements are satisfied.

To use the Run MySQL Drop Database workflow:

1. Create a deployable copy of the workflow.
2. Determine the values that you will specify for the parameters.

Note: There are no mandatory parameters required to run this workflow. All parameters are optional. You may need to expose additional parameters depending on your objectives.

3. In the workflow editor, expose any additional parameters that you need. You will specify values for those parameters when you create the deployment or at runtime.
4. Save the changes to the workflow (click **Save** in the lower right corner).
5. Create a new deployment.
6. On the Parameters tab, specify values (or set the type to Runtime Value) for the required parameters listed in step 2 and any additional parameters that you have exposed. You do not need to specify values for those parameters whose default values are appropriate for your environment.
7. On the Targets tab, specify one or more targets for this deployment.
8. Save the deployment (click **Save** in the lower right corner).
9. Run the workflow using this deployment, specifying any runtime parameters.

To verify the results:

The workflow will complete and report SUCCESS on the Console if it has run successfully. If an error occurs during workflow execution, the error is logged, and the workflow terminates in the FAILURE state. The database will be removed from the DMA environment section upon SUCCESS as well.

Parameters for MySQL - Drop Database

There are no mandatory parameters required to run this workflow. All parameters are optional. Some of these parameters are not initially visible in a deployment. For most parameters, if you do not specify a value for a parameter, a default value is assigned.

MySQL - Install Instance

The MySQL - Install Instance workflow installs software for MySQL 5.6 Enterprise x64 edition on RedHat Linux 6. This includes the server, client files, and any other optional components included in RPM files.

To use this workflow in your environment, see the following information:

Topic	Information Included
"Prerequisites for this Workflow" on the next page	List of prerequisites that must be satisfied before you can run this workflow
"How this Workflow Works" on page 242	Information about what the workflow does, including validation checks performed, steps executed, and step descriptions
" How to Run this Workflow" on page 243	Instructions for running this workflow in your environment
"Parameters for MySQL - Install Instance" on page 245	List of input parameters for this workflow

Prerequisites for this Workflow

Be sure that the following prerequisites are satisfied before you run the MySQL - Install Instance workflow:

- This solution requires DMA version 10.50.001.000 (or later).

The latest DMA solution packs require the latest DMA platform. To use the latest solution packs, update the DMA platform. DMA10.50.001.000 solution packs are supported on DMA10.50.001.000 (and later).

- You have installed the Database Provisioning solution pack.
- SE linux must be turned off.
- RPM files must be mounted locally, available through an external download server, or a combination of both.

The information presented here assumes the following: show assumptions

- DMA is installed and operational.
- At least one suitable target server (database) is available.
- You are logged in to the DMA web interface.
- You have permission to create, edit, and deploy copies of the workflows included in this solution pack.

For more information about prerequisites for MySQL database, refer to the [MySQL Server Documentation](#).

How this Workflow Works

This workflow installs software for MySQL 5.6 Enterprise x64 edition on RedHat Linux 6.

Steps Executed by the Workflow

The MySQL - Install Instance workflow includes the following steps. Each step must complete successfully before the next step can start. If a step fails, the workflow reports a failure and all subsequent steps are skipped.

Steps Used by MySQL - Install Instance

Workflow Step	Description
MySQL - Gather Parameters for Install Instance	This step gathers parameters to install software for MySQL - Install Instance workflow.
MySQL - Gather Advanced Parameters for Install Instance	This steps accepts parameters for advanced MySQL install server and sets defaults.
MySQL - Prepare Install Instance	This step prepares server for MySQL instance installation.
MySQL - Install Instance	This step installs list of RPMs to create a MySQL instance.
Download Software	This step automates the transfer of files from the HP SA Software Library to individual managed servers for use in downstream workflow steps. Verifies checksum of each file transferred.
MySQL - Verify Install Instance	This step verifies that MySQL and its components were installed correctly.
Cleanup Downloaded Files v2	This step removes all downloaded files and archives.
Discover MySQL Databases	This step discovers the MySQL instances and databases on the target machine.

How to Run this Workflow

The following instructions show you how to customize and run the MySQL - Install Instance workflow in your environment.

The workflow provides default values for some parameters. These default values are usually sufficient for a "typical" installation. You can override the defaults by specifying parameter values in the deployment. You can also expose additional parameters in the workflow, if necessary, to accomplish more advanced scenarios. Any parameters not explicitly specified in the deployment will have the default values listed in ["Parameters for MySQL - Install Instance" on page 245](#).

Note: Before following this procedure, review the ["Prerequisites for this Workflow" on page 241](#), and ensure that all requirements are satisfied.

To use the MySQL - Install Instance workflow:

1. Create a deployable copy of the workflow.
2. Determine the values that you will specify for the parameters.

Note: There are no mandatory parameters required to run this workflow. All parameters are optional. You may need to expose additional parameters depending on your objectives.
3. In the workflow editor, expose any additional parameters that you need. You will specify values for those parameters when you create the deployment or at runtime.
4. Save the changes to the workflow (click **Save** in the lower right corner).
5. Create a new deployment.
6. On the Parameters tab, specify values (or set the type to Runtime Value) for the required parameters listed in step 2 and any additional parameters that you have exposed. You do not need to specify values for those parameters whose default values are appropriate for your environment.
7. On the Targets tab, specify one or more targets for this deployment.
8. Save the deployment (click **Save** in the lower right corner).
9. Run the workflow using this deployment, specifying any runtime parameters.

To verify the results:

The workflow will complete and report SUCCESS on the Console if it has run successfully. If an error occurs during workflow execution, the error is logged, and the workflow terminates in the FAILURE state. The database will be removed from the DMA environment section upon SUCCESS as well.

To verify that MySQL process is running after the workflow is successfully completed, run the command **ps aux | grep mysql**.

Parameters for MySQL - Install Instance

The following tables describe the required and optional input parameters for this workflow. Some of these parameters are not initially visible in a deployment. For most parameters, if you do not specify a value for a parameter, a default value is assigned.

Parameters Defined in this Step: MySQL - Gather Parameters for Install Instance

Parameter Name	Default Value	Required	Description
List of RPMs	no default	required	Comma-delimited list of RPMs that are either available in the staging directory or will need to be downloaded from the software repository.

Parameters Defined in this Step: MySQL - Gather Advanced Parameters for Install Instance

Parameter Name	Default Value	Required	Description
Backup Zipfile	no default	optional	ZIP file to be used for installing the backup utility.
MySQL Root Password	no default	optional	Password for the MySQL user.
Staging Director	/tmp/mysql_stage	optional	Fully qualified path of the directory where MySQL installer will be downloaded to. Will be cleaned up at end of workflow execution. Default directory /tmp/mysql_stage will be created if no input is provided.
Template File	no default	optional	A template file to be used for custom configurations.

MySQL - Create Database

The MySQL - Create Database workflow creates a MySQL database and to add it to the DMA environment.

To use this workflow in your environment, see the following information:

Topic	Information Included
"Prerequisites for this Workflow" on the next page	List of prerequisites that must be satisfied before you can run this workflow
"How this Workflow Works" on page 248	Information about what the workflow does, including validation checks performed, steps executed, and step descriptions
" How to Run this Workflow" on page 249	Instructions for running this workflow in your environment
"Parameters for MySQL - Create Database" on page 251	List of input parameters for this workflow

Prerequisites for this Workflow

Be sure that the following prerequisites are satisfied before you run the MySQL - Create Database workflow:

- This solution requires DMA version 10.50.001.000 (or later).

The latest DMA solution packs require the latest DMA platform. To use the latest solution packs, update the DMA platform. DMA10.50.001.000 solution packs are supported on DMA10.50.001.000 (and later).

- You have installed the Database Provisioning solution pack.
- An existing MySQL instance to be used as the target instance.

The information presented here assumes the following: show assumptions

- DMA is installed and operational.
- At least one suitable target server (database) is available.
- You are logged in to the DMA web interface.
- You have permission to create, edit, and deploy copies of the workflows included in this solution pack.

For more information about prerequisites for MySQL database, refer to the [MySQL Server Documentation](#).

How this Workflow Works

This workflow performs the following actions:

- Creates a MySQL database and to add it to the DMA environment.

Steps Executed by the Workflow

The MySQL - Create Database workflow includes the following steps. Each step must complete successfully before the next step can start. If a step fails, the workflow reports a failure and all subsequent steps are skipped.

Steps Used by MySQL - Create Database

Workflow Step	Description
MySQL - Gather Parameters for Create Database	This step gathers parameters to install software for MySQL - Create Database workflow.
MySQL - Create Database	This steps accepts parameters for advanced MySQL install server and sets defaults.
Discover MySQL Databases	This step prepares server for MySQL instance installation.

How to Run this Workflow

The following instructions show you how to customize and run the MySQL - Create Database workflow in your environment.

The workflow provides default values for some parameters. These default values are usually sufficient for a "typical" installation. You can override the defaults by specifying parameter values in the deployment. You can also expose additional parameters in the workflow, if necessary, to accomplish more advanced scenarios. Any parameters not explicitly specified in the deployment will have the default values listed in ["Parameters for MySQL - Create Database" on page 251](#).

Note: Before following this procedure, review the ["Prerequisites for this Workflow" on page 247](#), and ensure that all requirements are satisfied.

To use the MySQL - Create Database workflow:

1. Create a deployable copy of the workflow.
2. Determine the values that you will specify for the parameters.

Note: There are no mandatory parameters required to run this workflow. All parameters are optional. You may need to expose additional parameters depending on your objectives.
3. In the workflow editor, expose any additional parameters that you need. You will specify values for those parameters when you create the deployment or at runtime.
4. Save the changes to the workflow (click **Save** in the lower right corner).
5. Create a new deployment.
6. On the Parameters tab, specify values (or set the type to Runtime Value) for the required parameters listed in step 2 and any additional parameters that you have exposed. You do not need to specify values for those parameters whose default values are appropriate for your environment.
7. On the Targets tab, specify one or more targets for this deployment.
8. Save the deployment (click **Save** in the lower right corner).
9. Run the workflow using this deployment, specifying any runtime parameters.

To verify the results:

The workflow will complete and report SUCCESS on the Console if it has run successfully. If an error occurs during workflow execution, the error is logged, and the workflow terminates in the FAILURE state. The database will be removed from the DMA environment section upon SUCCESS as well.

To display a list of databases, including the newly created one, run the command **show databases** within the MySQL program.

Parameters for MySQL - Create Database

The following tables describe the required and optional input parameters for this workflow. Some of these parameters are not initially visible in a deployment. For most parameters, if you do not specify a value for a parameter, a default value is assigned.

Parameters Defined in this Step: MySQL - Gather Parameters for Create Database

Parameter Name	Default Value	Required	Description
Database Name	no default	required	The name of the database to be created.
MySQL Password	no default	optional	The password for the specified MySQL user, this is valid only if used in conjunction with the MySQL user.
MySQL Unix User	no default	optional	The UNIX user that owns the MySQL daemon.
MySQL Username	no default	optional	The username for the MySQL user. This is not required if the .my.cnf file is configured for the instance user.
Web Service Password	no default	required	The password for the discovery web service API.
Web Service URL	no default	required	The URL for the discovery web service API.
Web Service User	no default	required	The user capable of modifying the managed environment through the discovery web service API.

MySQL - Start or Stop

The MySQL - Start or Stop workflow starts or stops an existing MySQL daemon.

To use this workflow in your environment, see the following information:

Topic	Information Included
"Prerequisites for this Workflow" on the next page	List of prerequisites that must be satisfied before you can run this workflow
"How this Workflow Works" on page 254	Information about what the workflow does, including validation checks performed, steps executed, and step descriptions
" How to Run this Workflow" on page 255	Instructions for running this workflow in your environment
"Parameters for MySQL - Start or Stop" on page 257	List of input parameters for this workflow

Prerequisites for this Workflow

Be sure that the following prerequisites are satisfied before you run the MySQL - Start or Stop workflow:

- This solution requires DMA version 10.50.001.000 (or later).

The latest DMA solution packs require the latest DMA platform. To use the latest solution packs, update the DMA platform. DMA10.50.001.000 solution packs are supported on DMA10.50.001.000 (and later).

- You have installed the Database Provisioning solution pack.
- Must target an existing MySQL instance.

The information presented here assumes the following: show assumptions

- DMA is installed and operational.
- At least one suitable target server (database) is available.
- You are logged in to the DMA web interface.
- You have permission to create, edit, and deploy copies of the workflows included in this solution pack.

For more information about prerequisites for MySQL database, refer to the [MySQL Server Documentation](#).

How this Workflow Works

This workflow performs the following actions:

- Starts or stops an existing MySQL daemon.

Steps Executed by the Workflow

The MySQL - Start or Stop workflow includes the following steps. Each step must complete successfully before the next step can start. If a step fails, the workflow reports a failure and all subsequent steps are skipped.

Steps Used by MySQL - Start or Stop

Workflow Step	Description
MySQL - Gather Parameters for Start or Stop	This step gathers parameters to install software for MySQL - Start or Stop workflow.
MySQL - Gather Advanced Parameters for Start or Stop	This step gathers advanced parameters for MySQL - Start or Stop workflow and sets defaults.
MySQL - Check Status	This steps checks the status of the MySQL to ensure that it matches Desired Status in the input parameter.
MySQL - Start or Stop	This step starts or stops an existing MySQL daemon, based on the value set for the parameter "Action".

How to Run this Workflow

The following instructions show you how to customize and run the MySQL - Start or Stop workflow in your environment.

The workflow provides default values for some parameters. These default values are usually sufficient for a "typical" installation. You can override the defaults by specifying parameter values in the deployment. You can also expose additional parameters in the workflow, if necessary, to accomplish more advanced scenarios. Any parameters not explicitly specified in the deployment will have the default values listed in ["Parameters for MySQL - Start or Stop" on page 257](#).

Note: Before following this procedure, review the ["Prerequisites for this Workflow" on page 253](#), and ensure that all requirements are satisfied.

To use the MySQL - Start or Stop workflow:

1. Create a deployable copy of the workflow.
2. Determine the values that you will specify for the parameters.

Note: There are no mandatory parameters required to run this workflow. All parameters are optional. You may need to expose additional parameters depending on your objectives.
3. In the workflow editor, expose any additional parameters that you need. You will specify values for those parameters when you create the deployment or at runtime.
4. Save the changes to the workflow (click **Save** in the lower right corner).
5. Create a new deployment.
6. On the Parameters tab, specify values (or set the type to Runtime Value) for the required parameters listed in step 2 and any additional parameters that you have exposed. You do not need to specify values for those parameters whose default values are appropriate for your environment.
7. On the Targets tab, specify one or more targets for this deployment.
8. Save the deployment (click **Save** in the lower right corner).
9. Run the workflow using this deployment, specifying any runtime parameters.

To verify the results:

The workflow will complete and report SUCCESS on the Console if it has run successfully. If an error occurs during workflow execution, the error is logged, and the workflow terminates in the FAILURE state. The database will be removed from the DMA environment section upon SUCCESS as well.

To verify MySQL daemon is indeed started/stopped based on workflow's outcome, run the command **service mysql status**.

Parameters for MySQL - Start or Stop

The following tables describe the required and optional input parameters for this workflow.

Parameters Defined in this Step: MySQL - Gather Parameters for Start or Stop

Parameter Name	Default Value	Required	Description
Action	no default	required	If set to "Start", the MySQL daemon will be started. If set to "Stop", the MySQL daemon will be stopped.

Oracle

The following topics are included:

Workflow type	Workflow name
Compliance	"Oracle - Compliance Audit v2" on page 260
Patching	"Oracle - Patch Home and Databases v5" on page 275
	"Oracle - Rollback Patch from Home and Databases v2" on page 283
	"Apply Oracle Patchset" on page 295
	"Clone Oracle Home" on page 311
	"Migrate Oracle Home" on page 320
	"Oracle - Migrate and Patch Grid Managed Database" on page 331
	"Oracle - Patch Grid Infrastructure and Databases v6" on page 341
	"Oracle - Rollback Patch from Grid Infrastructure and Database" on page 361
Refreshing	"Oracle - Extract Database via RMAN" on page 373
	"Oracle - Refresh Database via RMAN" on page 384
	"Oracle - Extract and Refresh Database via RMAN" on page 396
	"Oracle - Export Database via Data Pump" on page 410
	"Oracle - Refresh Database via Data Pump" on page 427
	"Oracle - Migrate Database TTS" on page 444

Workflow type	Workflow name
Provisioning	"Oracle - Drop Database" on page 456
	"Oracle - Provision Data Guard v6" on page 462
	"Oracle - Create Data Guard Broker Configuration" on page 472
	"Oracle - Configure Data Guard Broker Properties" on page 480
	"Oracle - Data Guard Broker Switchover" on page 488
	"Oracle - Provision or Upgrade Grid Infrastructure" on page 524
	"Oracle - Provision Database Software v2" on page 533
	"Oracle - Provision Database v3" on page 541
	Oracle - Upgrade Database v2
	"Provisioning Grid Infrastructure" on page 495
	"Provisioning RAC" on page 523
	Oracle - Provision Pluggable Database
Release Management	"Oracle - SQL Release v3" on page 551

Oracle - Compliance Audit v2

The Oracle - Compliance Audit v2 workflow enables you to audit an Oracle Database instance for compliance with one of the following security benchmarks:

- Center for Internet Security (CIS) security configuration benchmarks
- Payment Card Industry (PCI) data security standard
- Sarbanes-Oxley (SOX) requirements

The workflow performs CIS Level 1 and Level 2 auditing and can identify more than 175 compliance related problems.

The workflow performs the checks included in the CIS benchmark and then maps those CIS checks to the benchmark type that you specify in the Compliance Type parameter. The audit summary email will match the Compliance Type that you specify.

To use this workflow in your environment, see the following information:

Topic	Information Included
"Prerequisites for this Workflow" on the next page	List of prerequisites that must be satisfied before you can run this workflow
"How this Workflow Works"	Information about what the workflow does, including validation checks performed, steps executed, and a step descriptions
"How to Run this Workflow"	Instructions for running this workflow in your environment
"Sample Scenarios"	Examples of typical parameter values for this workflow
Parameters	List of input parameters for this workflow

Prerequisites for this Workflow

Be sure that the following prerequisites are satisfied before you run the Oracle - Compliance Audit workflow:

- The latest Replace...DMA solution packs require the latest Replace...DMA platform. To use the latest solution packs, update the DMA platform. Replace...DMA 10.50.000.000 solution packs are supported on DMA 10.50.000.000 (and later).
- You have installed the Database Compliance solution pack.

For more information about prerequisites for Oracle database, refer to the [Oracle Server Documentation](#).

How this Workflow Works

This workflow performs the following actions:

1. Prepares to run the workflow by gathering information about the target Oracle Database instance and validating parameter values.
2. Audits the various configuration settings specified in the pertinent benchmark.
3. Composes and sends an email containing the results of the audit.

Note: The emails are sent through the mail server configured on the DMA server. You can configure the mail server in the path below:

DMA setup > Configuration > Outgoing Mail > Server.

Validation Checks Performed

This workflow validate the following conditions:

1. The Oracle Home derived in the Get Oracle Home step is a fully qualified path that exists on the target server.
2. The workflow can connect to the Oracle SID derived in the Get Oracle Home step.
3. Any Excluded Checks specified by the user refer to actual CIS checks.
4. Any email addresses specified are valid addresses.
5. The workflow can create the temporary file that will store the compliance check results.

Steps Executed

The "Oracle - Compliance Audit v2" workflow includes the following steps. Each step must complete successfully before the next step can start. If a step fails, the workflow reports a failure and all subsequent steps are skipped.

Steps Used in Oracle Compliance Audit

Workflow Step	Description
Gather Parameters for Oracle Compliance	<p>This step gathers three pieces of information that the workflow needs to perform the compliance audit:</p> <ul style="list-style-type: none"> • The type of compliance audit to perform (CIS, PCI, or SOX) • A list of compliance checks to exclude from the audit (if any) • The location of the Oracle inventory files. <p>All parameters are optional.</p>
Gather Advanced Parameters for Oracle	<p>This step gathers the information that the workflow needs to create and deliver the compliance audit report via email. It also enables you</p>

Steps Used in Oracle Compliance Audit, continued

Workflow Step	Description
Compliance v2	to specify the name of the most recent Oracle patch that was applied to the pertinent Oracle Home (derived from the Oracle inventory file).
Validate Compliance Parameters v2	<p>This step validates the input parameters specified in the previous steps. It validates the list of excluded checks to ensure that all specified checks in the list correspond to actual Center for Internet Security (CIS) benchmark items. It also validates the email information to ensure that all specified email addresses are valid.</p> <p>The step then creates the path to the temporary file that will store the results of the current audit as the workflow is running. This file is deleted after the audit report is sent.</p>
Prepare Server	This step prepares the Server Wrapper and Instance Wrapper, which enable subsequent steps to be executed by the OS administrator user or the owner of the database or middleware software.
Get Oracle Home	This step determines the value of ORACLE_HOME from the Oracle inventory file on UNIX targets or from the Registry on Windows targets.
Prepare Oracle Instance	This step gathers the information that the workflow will need to access the pertinent Oracle instance.
Get Listener Names	<p>This step gets the names of the Oracle listeners that are running.</p> <p>Results can be filtered based on one or more ORACLE_HOMEs, one or more ORACLE_SIDs, or both.</p>
Database Installation and Patching Requirements	This step audits the scorable recommendations in Section 1, Oracle Database Installation and Patching Requirements, of the CIS Security Benchmarks for Oracle.
Audit Oracle Parameter Settings v2	This step audits the scorable recommendations in Section 2, Oracle Parameter Settings, of the CIS Security Benchmarks for Oracle.
Oracle Connection and Login Restrictions	This step audits the scorable recommendations in Section 3, Oracle Connection and Login Restrictions, of the CIS Security Benchmarks for Oracle.
Audit Oracle User Access and Authorization Restrictions	This step audits the scorable recommendations in Section 4, Audit Oracle User Access and Authorization Restrictions, of the CIS Security Benchmarks for Oracle.
Audit Logging Policies and Procedures	This step audits the scorable recommendations in Section 5, Audit Logging Policies and Procedures, of the CIS Security Benchmarks for Oracle.
Validate Post Compliance Checks	This step reads the temporary file that contains the results of the compliance audit and prints the audit results to the DMA Console. If email addresses were specified, it also creates a report in HTML format that will be emailed to those addresses by a later step in the workflow.
Send Compliance Email v2	If email addresses are provided, this step sends the previously generated compliance audit report to the specified email addresses.
Delete File	This step deletes the specified file on the target server.

Note: For input parameter descriptions and defaults, see "[Parameters for Oracle - Compliance Audit](#)" on page 272.

How to Run this Workflow

The following instructions show you how to customize and run the ["Oracle - Compliance Audit v2"](#) workflow in your environment.

The workflow provides default values for some parameters. These default values are usually sufficient for a "typical" installation. You can override the defaults by specifying parameter values in the deployment. You can also expose additional parameters in the workflow, if necessary, to accomplish more advanced scenarios. Any parameters not explicitly specified in the deployment will have the default values listed in ["Parameters for Oracle - Compliance Audit" on page 272](#).

Note: Before following this procedure, review the ["Prerequisites for this Workflow" on page 261](#), and ensure that all requirements are satisfied.

To use the Run Oracle Compliance Audit workflow:

1. Create a deployable copy of the workflow.
2. Determine the values that you will specify for the following parameters:

Parameters Defined in this Step: Gather Parameters for Oracle Compliance

Parameter Name	Default Value	Required	Description
Compliance Type	CIS	optional	Type of compliance report that will be generated by the workflow. Supported types are: CIS = Center for Internet Security (CIS) Security Configuration Benchmark PCI = Payment Card Industry (PCI) Data Security Standard SOX = Sarbanes-Oxley (SOX) sections 302.2, 302.4b, 302.4c, and 302.5 requirements
Excluded Compliance Checks	no default	optional	Comma-separated list of compliance checks to exclude from the audit. For example: 1.2, 2, 3.*, 5*, 6.1.2 Note: Make sure that the checks specified here correspond with the compliance audit type (CIS, PCI, or SOX) that you are running.
Inventory Files	see description	optional	Comma-separated list of fully qualified Oracle inventory files. If this parameter is not specified, it defaults to one of the following values: Linux or AIX: /etc/oraInst.loc Solaris: /var/opt/oracle/oraInst.loc Windows: %ProgramFiles%\Oracle\Inventory

Parameters Defined in this Step: Gather Advanced Parameters for Oracle Compliance

Parameter Name	Default Value	Required	Description
Email Addresses to Receive Report	no default	optional	Comma-separated list of email addresses for those individuals or groups who will receive a copy of the compliance audit report.

Note: This is the minimum set of parameters required to run this workflow. You may need to expose additional parameters depending on your objectives.

See ["Parameters for Oracle - Compliance Audit" on page 272](#) for detailed descriptions of all input parameters for this workflow, including default values.

3. In the workflow editor, expose any additional parameters that you need. You will specify values for those parameters when you create the deployment.
4. Save the changes to the workflow (click **Save** in the lower right corner).
5. Create a new deployment.
6. On the Parameters tab, specify values for the required parameters listed in step 2 and any additional parameters that you have exposed. You do not need to specify values for those parameters whose default values are appropriate for your environment.
7. On the Targets tab, specify one or more targets for this deployment.
8. Save the deployment (click **Save** in the lower right corner).
9. Run the workflow using this deployment .

To verify the results:

The workflow will complete and report SUCCESS on the Console if it has run successfully. If an error occurs during workflow execution, the error is logged, and the workflow terminates in the FAILURE state.

Information about each compliance check is displayed in the step output on the Console (and the History page) for each of the auditing steps. A summary of the compliance audit is also displayed in the step output for the Validate Post-Compliance Checks step.

To view the reports:

A compliance audit summary in HTML format is emailed to all parties on the Email Addresses to Receive Report list.

After you run this workflow, you can generate two types of compliance reports on the Reports page:

- Database Compliance Report
- Database Compliance Detail Report

To access the Database Compliance reports:

1. Go to the Reports page.
2. At the bottom of the page, specify the following settings:

For the Database Compliance Report:

- a. Select the Database Compliance report.
- b. Select the organization where your target resides.
- c. Because this report lists the latest compliance audit reports for all targets in the specified organization, you do not specify a Server, Database, or Time span.

For the Database Compliance Detail Report:

- a. Select the Database Compliance Details report.
- b. Select the organization where your target resides.
- c. Specify the Server and Instance that you selected when you created your deployment.

3. Click **Run report**.

Sample Scenarios

This topic shows you how to use various parameters to achieve the following compliance audit scenarios in your environment using the "Oracle - Compliance Audit v2" workflow.

Scenario 1: Perform a Partial CIS Compliance Audit and Email the Results

In the scenario, the following checks are excluded from the audit:

- Section 8: Oracle Profile (User) Setup Settings
- Section 9: Oracle Profile (User) Access Settings

A summary report is sent to the three parties listed in the Email Addresses to Receive Report parameter.

Parameter Name	Example Value	Description
Compliance Type	CIS	<p>Type of compliance report that will be generated by the workflow. Supported types are:</p> <p>CIS = Center for Internet Security (CIS) Security Configuration Benchmark</p> <p>PCI = Payment Card Industry (PCI) Data Security Standard</p> <p>SOX = Sarbanes-Oxley (SOX) sections 302.2, 302.4b, 302.4c, and 302.5 requirements</p>
Excluded Compliance Checks	8.*,9.*	<p>Comma-separated list of compliance checks to exclude from the audit. For example:</p> <p>1.2, 2, 3.*, 5*, 6.1.2</p> <p>Note: Make sure that the checks specified here correspond with the compliance audit type (CIS,</p>

Parameter Name	Example Value	Description
		PCI, or SOX) that you are running.

Note: Some of these parameters are not exposed by default in the deployment.

Be sure that the default values for all remaining input parameters are appropriate for your environment (see ["Parameters for Oracle - Compliance Audit" on page 272](#)).

Scenario 2: Perform a Full PCI Compliance Audit and Email the Results

In the scenario, no checks are excluded from the audit. A summary report is sent to the three parties listed in the Email Addresses to Receive Report parameter.

Parameter Name	Example Value	Description
Compliance Type	PCI	Type of compliance report that will be generated by the workflow. Supported types are: CIS = Center for Internet Security (CIS) Security Configuration Benchmark PCI = Payment Card Industry (PCI) Data Security Standard SOX = Sarbanes-Oxley (SOX) sections 302.2, 302.4b, 302.4c, and 302.5 requirements
Email Addresses to Receive Report	DBAdminTeam@mycompany.com, DBAdminMgr@mycompany.com, CustomerSupportTeam@mycompany.com	Comma-separated list of email addresses for those individuals or groups who will receive a copy of the compliance audit report.

Note: Some of these parameters are not exposed by default in the deployment.

Be sure that the default values for all remaining input parameters are appropriate for your environment (see ["Parameters for Oracle - Compliance Audit" on page 272](#)).

Scenario 3: Perform a Full SOX Compliance Audit and Email the Results

In the scenario, no checks are excluded from the audit. A summary report is sent to the three parties listed in the Email Addresses to Receive Report parameter.

Parameter Name	Example Value	Description
Compliance Type	SOX	Type of compliance report that will be generated by the workflow. Supported types are: CIS = Center for Internet Security (CIS) Security Configuration Benchmark PCI = Payment Card Industry (PCI) Data Security Standard SOX = Sarbanes-Oxley (SOX) sections 302.2, 302.4b, 302.4c, and 302.5 requirements
Email Addresses to Receive Report	DBAdminTeam@mycompany.com, DBAdminMgr@mycompany.com, CustomerSupportTeam@mycompany.com	Comma-separated list of email addresses for those individuals or groups who will receive a copy of the compliance audit report.

Note: Some of these parameters are not exposed by default in the deployment.

Be sure that the default values for all remaining input parameters are appropriate for your environment (see ["Parameters for Oracle - Compliance Audit" on page 272](#)).

Scenario 4: Perform a Full CIS Compliance Audit and Display the Results on the DMA Console

In the scenario, all scorable checks are performed, and the compliance audit report is displayed only on the DMA Console. In this case, a summary report is not emailed. This scenario would be appropriate for initial testing.

It is not necessary to specify any input parameters in this scenario unless the Oracle Databaseinventory file is located in a non-standard directory.

Parameter Name	Example Value	Description
Compliance Type	CIS	Type of compliance report that will be generated by the workflow. Supported types are: CIS = Center for Internet Security (CIS) Security Configuration Benchmark PCI = Payment Card Industry (PCI) Data Security Standard SOX = Sarbanes-Oxley (SOX) sections 302.2, 302.4b, 302.4c, and 302.5 requirements

Be sure that the default values for all remaining input parameters are appropriate for your environment (see ["Parameters for Oracle - Compliance Audit" on the next page](#)).

Parameters for Oracle - Compliance Audit

The following tables describe the required and optional input parameters for this workflow. Some of these parameters are not initially visible in a deployment. For most parameters, if you do not specify a value for a parameter, a default value is assigned.

Note: Only those parameters that are configurable in a standard deployment are listed here. Input parameters that must be mapped to output parameters of previous steps are not listed.

Parameters Defined in this Step: Gather Parameters for Oracle Compliance

Parameter Name	Default Value	Required	Description
Compliance Type	CIS	optional	Type of compliance report that will be generated by the workflow. Supported types are: CIS = Center for Internet Security (CIS) Security Configuration Benchmark PCI = Payment Card Industry (PCI) Data Security Standard SOX = Sarbanes-Oxley (SOX) sections 302.2, 302.4b, 302.4c, and 302.5 requirements
Excluded Compliance Checks	no default	optional	Comma-separated list of compliance checks to exclude from the audit. For example: 1.2, 2, 3.*, 5*, 6.1.2 Note: Make sure that the checks specified here correspond with the compliance audit type (CIS, PCI, or SOX) that you are running.
Inventory Files	see description	optional	Comma-separated list of fully qualified Oracle inventory files. If this parameter is not specified, it defaults to one of the following values:

Parameters Defined in this Step: Gather Advanced Parameters for Oracle Compliance

Parameter Name	Default Value	Required	Description
Email Addresses to Receive Report	no default	optional	Comma-separated list of email addresses for those individuals or groups who will receive a copy of the compliance audit report.
Latest Patch	no default	optional	Most recent Oracle patch installed on this Oracle Home.

Patching Database

This solution pack contains the following workflows:

Workflow Template	Description
Oracle - Patch Home and Databases	This workflow applies an Oracle Critical Patch Update or Security Patch Update (CPU/SPU), Patch Bundle, or Patch Set Update (PSU) to an Oracle Home and to the Oracle Database Instances associated with the Oracle Home. It also updates the OPatch version if the OPatch Archive file is specified.
Oracle - Rollback Patch from Home and Databases	This workflow rolls back a Critical Patch Update or Security Patch Update (CPU/SPU), Patch Bundle, or Patch Set Update (PSU) from an Oracle Home and from the Oracle Database Instances associated with the Oracle Home.
Apply Oracle Patchset	This workflow applies an Oracle Software Patch Set to an existing Oracle Home and Oracle Database.
Clone Oracle Home	This workflow makes a clone (copy) of an Oracle Home on the same server.
Migrate Oracle Home	This workflow moves an Oracle Instance from one Oracle Home to another Oracle Home.

Each workflow included in this solution pack has a set of input parameters whose values will be unique to your environment. If you provide correct values for the parameters that each scenario requires, the workflow will be able to accomplish its objective.

There are two steps required to customize this solution:

1. Ensure that all required parameters are visible. You do this by using the workflow editor.

For simple patching scenarios, you can use the default values for most parameters. To use this solution's more advanced features, you will need to expose additional parameters.

2. Specify the values for those parameters. You do this when you create a deployment.

Tip: Detailed instructions are provided in the "How to Run this Workflow" topic for each workflow.

The information presented here assumes the following:

- DMA is installed and operational.
- At least one suitable target server is available.
- You are logged in to the DMA web interface.
- You have permission to create, edit, and deploy copies of the workflows included in this solution

pack.

Tip: All parameters used by the workflows in this solution are provided in the "Parameters" topic associated with each workflow.

Oracle - Patch Home and Databases v5

This workflow applies an Oracle patch to an Oracle home and database. It also updates the OPatch version if the OPatch archive file is specified. This workflow only applies to single instance installations. It is not designed for Oracle Real Application Clusters (RAC).

This workflow applies the following patch types to Oracle home and database on different platforms as supported by Oracle.

- Critical Patch Update(CPU) / Security Patch Update (SPU)
- Patch Set Update (PSU)
- Interim Patch/One-off Patch
- Oracle JavaVM Component PSU (OJVM)
- Combo Patches (CPU+OJVM/ PSU+OJVM)
- Bundle Patch

This workflow stops all processes running from the ORACLE_HOME in order to patch. This includes the Listener, which may be servicing instances outside this ORACLE_HOME. If multiple patch types are provided as input, the patches will be applied in the following order:

1. CPU
2. PSU
3. OJVM
4. Interim

To use this workflow in your environment, see the following information:

Topic	Information Included
"Prerequisites for this Workflow" on the next page	List of prerequisites that must be satisfied before you can run this workflow
"How this Workflow Works" on page 278	Information about what the workflow does, including validation checks performed, steps executed, and step descriptions
"How to Run this Workflow" on page 280	Instructions for running this workflow in your environment
"Parameters for Oracle - Patch Home and Databases" on page 281	List of input parameters for this workflow

Tip: To patch Server Automation Grid standalone environments, see *Achieve Patch Related Compliance for Oracle Grid Standalone Environments Using DMA*.

To patch more complex Oracle clustered environments, see *Achieve Patch Related Compliance for Oracle RAC Environments Using DMA*.

These documents are available at: softwaresupport.hp.com

Prerequisites for this Workflow

Be sure that the following prerequisites are satisfied before you run this workflow:

- The Oracle Home and database are ready to be updated.
- The DMA server is online.
- You have obtained the following files:
 - The patch archive from Oracle
 - The current OPatch version from Oracle (optional)
- You have licenses for Oracle Database and DMA.
- You have coordinated a scheduled outage for all application servers that use the databases.
- You have read access to all specified inventory pointers (Linux/UNIX).
- You have enough free space available, which varies depending on the Oracle patch.

For more information about prerequisites for Oracle database, refer to the [Oracle Server Documentation](#).

How this Workflow Works

This workflow performs the following actions:

Applies Oracle quarterly patches on Oracle standalone environments and standalone dataguard.

Steps Executed by the Workflow

The Oracle - Patch Home and Databases v5 workflow includes the following steps. Each step must complete successfully before the next step can start. If a step fails, the workflow reports a failure and all subsequent steps are skipped.

Steps Used by Oracle - Patch Home and Databases v5

Workflow Step	Description
Gather Parameters for Patch Home and Database	This step gathers parameters for the Oracle - Patch Home and Database workflow.
Gather Advanced Parameters for Patch Home and Database v2	This steps gathers advanced parameters for the Oracle - Patch Home and Database workflow.
Parse Oracle Inventory	<p>This step parses the Oracle inventory files that exists or forwards the inventory information does not exist.</p> <p>■ This step must be run as the DMA superuser.</p>
Validate Patch Home and Database v2	This step validates the parameters specified in Oracle – Patch Home and Database v3 workflow.
Download Software v2	This step automates the transfer of files from the HPE SA Software Library to individual managed servers for use in downstream workflow steps. This step also verifies checksum of each file transferred.
Oracle - Upgrade OPatch Utility	This step takes backup of the existing OPatch utility and updates the OPatch utility to the version provided as input.
Cleanup Downloaded Files v2	This step remove all downloaded files and archives.
Oracle - Unzip Patch Archives for Patch Oracle Home and Databases	This step unzips (extracts) the patch archives to the given folder.
Oracle - Parse Patch Information	<p>This step parses the patch archive and extracts the following information:</p> <ul style="list-style-type: none"> • OPatch Version required to apply the patch • Additional Patch Numbers • Database version on which the patch is applicable • Ignorable Oracle errors • Patch Type : SPU(or CPU), PSU, Combo, One-off, OJVM, Bundle • Patch Name
Oracle - Post Patch	This step validates whether patch that is being applied is already present

Steps Used by Oracle - Patch Home and Databases v5, continued

Workflow Step	Description
Unzip Validation	on the given Oracle home.
Run slibclean	This step runs the slibclean command on required operating systems.
Verify Oracle Versions	This step validates if the database version is same as the database version of the patch being applied. It also validates, if the OPatch utility is higher than the OPatch utility version recommended by Oracle.
Data Guard Prechecks v2	This step cancels Managed Recovery Process on the standby database.
Oracle - Stop Processes Standalone Target v3	This step stops all Oracle instances in a list, stops all Oracle listeners in the list, and attempts to stop the Oracle agent.
Cleanup Downloaded Files v2	This step removes all downloaded files and archives.
Oracle - Patch Standalone Target Homes	This step patches Oracle home directory using OPatch utility.
Oracle - Start Processes Standalone Target v3	This step starts all Oracle instances in a list, starts all Oracle listeners in the a list, and attempts to start Oracle agent.
Data Guard Postchecks	This step performs Managed Recovery Process (MRP) on the standby database.
Oracle - Patch Standalone Databases v3	This step applies patches for standalone databases.
Cleanup Downloaded Files v2	This step removes all downloaded files and archives.
Discover Oracle Databases	<p>This step audits the server's physical environment looking for Oracle instances and databases.</p> <p>Discovery is ONLY additive. It will not remove instances or databases currently in your environment. It is the end-user's responsibility to delete content that is no longer in use.</p> <p>In cluster situations where one node is active while other nodes are inactive, discovery will only find instances and databases on the active node.</p>

Note: For input parameter descriptions and defaults, see ["Parameters for Oracle - Patch Home and Databases" on page 281](#).

How to Run this Workflow

The following instructions show you how to customize and run the Oracle – Patch Home and Database v5 workflow in your environment.

The workflow provides default values for some parameters. These default values are usually sufficient for a "typical" installation. You can override the defaults by specifying parameter values in the deployment. You can also expose additional parameters in the workflow, if necessary, to accomplish more advanced scenarios. Any parameters not explicitly specified in the deployment will have the default values listed in ["Parameters for Oracle - Patch Home and Databases" on the next page](#).

Note: Before following this procedure, review the ["Prerequisites for this Workflow" on page 277](#), and ensure that all requirements are satisfied.

To use the Run Oracle – Patch Home and Database v5 workflow:

1. Create a deployable copy of the workflow.
2. Determine the values that you will specify for the parameters.

Note: There are no mandatory parameters required to run this workflow. All parameters are optional. You may need to expose additional parameters depending on your objectives.

See ["Parameters for Oracle - Patch Home and Databases" on the next page](#) for detailed descriptions of all input parameters for this workflow, including default values.

3. In the workflow editor, expose any additional parameters that you need. You will specify values for those parameters when you create the deployment or at runtime.
4. Save the changes to the workflow (click **Save** in the lower right corner).
5. Create a new deployment.
6. On the Parameters tab, specify values (or set the type to Runtime Value) for the required parameters listed in step 2 and any additional parameters that you have exposed. You do not need to specify values for those parameters whose default values are appropriate for your environment.
7. On the Targets tab, specify one or more targets for this deployment.
8. Save the deployment (click **Save** in the lower right corner).
9. Run the workflow using this deployment, specifying any runtime parameters.

To verify the results:

The workflow will complete and report SUCCESS on the Console if it has run successfully. If an error occurs during workflow execution, the error is logged, and the workflow terminates in the FAILURE state. The database will be removed from the DMA environment section upon SUCCESS as well.

Parameters for Oracle - Patch Home and Databases

The following tables describe the required and optional input parameters for this workflow. Some of these parameters may not be initially visible in a deployment. For some parameters, if you do not specify a value for a parameter, a default value is assigned.

Input Parameters Defined in this Step: Gather Parameters for Patch Home and Database

Parameter Name	Default Value	Required	Description
Oracle Home	no default	required	Absolute path of the Oracle home directory that is to be patched. Example: /u01/app/oracle/product/12.1.0/dbhome_1
Patch Archive	no default	required	Comma separated list of patch archives that needs to be applied on the Oracle home. Example: p22502456_112040_Linux-x86-64.zip, p14666816_112040_Linux-x86-64.zip

Input Parameters Defined in this Step: Gather Advanced Parameters for Patch Home and Database

Parameter Name	Default Value	Required	Description
Cleanup Downloaded Files	True	required	Value to represent whether the patch archive and extracted patch archive needs to be deleted after completion of the workflow. Valid values are True or False. Default is True.
Existing OPatch Backup Location	no default	required	Location to take backup of the existing OPatch directory. The backup of OPatch directory is taken only when the Patch Archive input parameter is specified. If no input is provided, the Oracle home directory is used for backup location. Oracle user must have write access to the directory specified.
Ignorable Oracle Errors	no default	optional	A comma-separated list of Oracle errors to be ignored when applying the patch to the database. This is in addition to the list of Oracle errors specified in the patch readme document. Values are of the form ORA-nnnnn.
Ignore SIDs	no default	optional	Comma separated SIDs to be ignored when applying the database patch.
Inventory Files	no default	optional	A comma-separated list of fully-qualified Oracle inventory files. If this parameter is not specified, the workflow looks for the oraInst.loc file in /etc and /var/opt/oracle folder.
OCM Response File	no default	optional	The path name of the Oracle Configuration Manager (OCM) response file. If not found on the target, this file is downloaded from the software directory on the SA. If left blank, a default response file will be created.

Input Parameters Defined in this Step: Gather Advanced Parameters for Patch Home and Database, continued

Parameter Name	Default Value	Required	Description
OPatch Archive	no default	optional	OPatch Archive to be applied on oracle home. Example: p6880880_112000_Linux-x86-64.zip.
OPatch Version	no default	optional	Version of the OPatch to be used for patching. This parameter has to be specified when OPatch version lower than the one specified in readme document of the Patch archive is to be used for patching.
Patch Download Location	/tmp	optional	Location where the patch archive has to be downloaded.
Patch Extraction Location	no default	optional	Location where the Patch archive will be extracted.
Preparatory SQL Script	no default	optional	File name containing SQL statements that must be run before the database catalog update. This file is passed directly to SQLPlus and must be formatted as such. If not found on the target, this file is downloaded from SA.
Recompile Invalid Objects	False	optional	Value to represent whether the utlrl.sql needs to be executed to recompile the invalid Java objects. Valid values are True or False. Default value is False.

Oracle - Rollback Patch from Home and Databases v2

This workflow rolls back a Critical Patch Update or Security Patch Update (CPU/SPU), Patch Bundle, or Patch Set Update (PSU) from an Oracle Home and from the Oracle Database instances associated with the Oracle Home.

Use this workflow if you encounter problems after applying a patch update. Only the last patch that was applied is rolled back.

For additional information about how the Oracle - Rollback Patch from Home and Databases workflow can be used with other patching workflows see How to Use the Workflows Together topic.

This workflow only applies to single Oracle Instance installations. It is not designed for Oracle Real Application Clusters (RAC).

If the Oracle patch has already been removed, this workflow will verify the patch removal and end with SUCCESS status.

Caution: This workflow stops all processes running from the ORACLE_HOME in order to patch. This includes the Oracle Listener, which may be servicing Oracle Instances outside this ORACLE_HOME.

To use this workflow in your environment, see the following information:

Topic	Information Included
"Prerequisites for this Workflow"	List of prerequisites that must be satisfied before you can run this workflow
"How this Workflow Works"	Information about what the workflow does, including validation checks performed, steps executed, and a high-level process flow
"How to Run this Workflow"	Instructions for running this workflow in your environment
"Sample Scenario"	Examples of typical parameter values for this workflow
Parameters	List of input parameters for this workflow

Note: The documentation for this workflow contains steps that are referred to by their base names. The names in the HPE DMA user interface may have a version appended, for example, v2.

Prerequisites for this Workflow

Be sure that the following prerequisites are satisfied before you run the ["Oracle - Rollback Patch from Home and Databases v2"](#) workflow:

- The latest DMA solution packs require the latest DMA platform. To use the latest solution packs, update the DMA platform. DMA 10.30 solution packs are supported on DMA 10.30 (and later).
- You have installed the DMA Database Patching Solution Pack.
- You have read access to all specified inventory pointers (Linux/UNIX).

Caution: This workflow stops all processes running from the ORACLE_HOME in order to rollback the patch. This includes the Oracle Listener, which may be servicing Oracle Instances outside this ORACLE_HOME.

For more information about prerequisites for Oracle Database, refer to the [Oracle Product Documentation](#).

How this Workflow Works

The following information describes how the "Oracle - Rollback Patch from Home and Databases v2" workflow works:

Overview

This workflow does the following things in the order shown:

- The initial steps of the workflow prepare it to roll back the last patch applied to the Oracle Home. The workflow processes user input parameters, constructs commands used in subsequent steps, and downloads any required files.
- The workflow rolls back the Critical Patch Update from the Oracle Database Home. The workflow stops all Oracle Instances, all Oracle Listeners in the list, and the Oracle Agent. The workflow removes any currently unused modules in kernel and library memory. Then the workflow runs the OPatch utility to roll back an Oracle supplied Patch and runs the Oracle provided `cpu_root.sh` script to complete the rollback.
- The final steps of the workflow allow the workflow to end cleanly. The workflow restarts all the Oracle Instances, all Oracle Listeners, and the Oracle Agent. Then it runs Discovery to update the metadata and cleans up the downloaded files.

Validation Checks Performed

Much of the validation centers on the input parameters:

- The input parameters have the proper syntax (no special characters or spaces).
- Files exist or have valid specifications.
- The supplied patch update applies to the current Oracle Database version.

Steps Executed

The Oracle - Rollback Patch from Home and Databases workflow includes the following steps. Each step must complete successfully before the next step can start. If a step fails, the workflow reports a failure and all subsequent steps are skipped.

Steps Used in Oracle - Rollback Patch from Home and Databases v2

Workflow Step	Description
Gather Parameters for Rollback Patch from Home and Databases v2	This step gathers the required parameters for the Oracle - Rollback Patch from Home and Databases workflow.
Gather Advanced Parameters for Rollback Patch from Home and Databases v2	This step gathers the optional advanced parameters for the Oracle - Rollback Patch from Home and Databases workflow.
Parse Oracle Inventory	<p>This step parses the specified Oracle inventory files (if they exist) and passes the inventory information to subsequent steps.</p> <ul style="list-style-type: none"> • If one or more Inventory Files are specified and they exist, the step parses these files and extracts their contents. • If no Inventory Files are specified, the step assigns the appropriate default and attempts to parse that file. • If one or more Inventory Files are specified and they do not exist, the step creates inventory information based on the specified Oracle Account and Oracle Home.
Validate Rollback Patch from Home and Databases v2	This step validates the specified values of the input parameters for the "Oracle - Rollback Patch from Home and Databases v2" workflow.
Download Software	This step downloads a list of files to a specified location on the target server.
Unzip for Rollback Patch Home and Databases	This step unzips the patch archive at the given location.
Oracle - Parse Patch Information	<p>This step parses the patch archive and extract the following information:</p> <ul style="list-style-type: none"> • OPatch version required to apply the patch • Additional patch numbers • Database version on which the patch is applicable • Ignorable Oracle errors • Patch Type : SPU (or CPU), PSU, Combo, One-off, OJVM, Bundle • Patch name
Cleanup Downloaded Files v2	This step removes all downloaded files and archives.
Run slibclean	This step runs the <code>slibclean</code> command on required targets. The <code>slibclean</code> utility removes any currently unused modules in kernel and library memory.

Steps Used in Oracle - Rollback Patch from Home and Databases v2, continued

Workflow Step	Description
Rollback Patch Home and Databases v2	This step rolls back the patch from the Oracle home and databases. If any preparatory SQL script is provided as input, then the same will be executed on each instance prior to rollback of the database patch. If recompile invalid object parameter is specified as true, then the utlrp.sql script will be executed after the database patch is rolled back.
Verify Home and Databases Patch Rolledback v2	This step validates if the patch has been rolled back.
Discover Oracle Databases	<p>This step audits the server's physical environment looking for Oracle instances and databases.</p> <p>Note: Discovery is ONLY additive. It will not remove instances or databases currently in your environment. It is the end-user's responsibility to delete content that is no longer in use.</p> <p>In cluster situations where one node is active while other nodes are inactive, Discovery will only find instances and databases on the active node. Nothing will be added to inactive nodes.</p>
Cleanup Downloaded Files v2	This step removes all downloaded files and archives.

For parameter descriptions and defaults, see ["Parameters for Oracle - Rollback Patch from Home and Databases" on page 293](#).

How to Run this Workflow

The following instructions show you how to customize and run the ["Oracle - Rollback Patch from Home and Databases v2"](#) workflow in your environment.

Tip: For detailed instructions to run DMA workflows—using the Oracle - Compliance Audit workflow as an example—see DMA Quick Start Tutorial.

The workflow provides default values for some parameters. These default values are usually sufficient for a "typical" installation. You can override the defaults by specifying parameter values in the deployment. You can also expose additional parameters in the workflow, if necessary, to accomplish more advanced scenarios. Any parameters not explicitly specified in the deployment will have the default values listed in ["Parameters for Oracle - Rollback Patch from Home and Databases"](#) on page 293.

Note: Before following this procedure, review the ["Prerequisites for this Workflow"](#) on page 284, and ensure that all requirements are satisfied.

To use the Oracle - Rollback Patch from Home and Databases workflow:

1. Create a deployable copy of the workflow.
2. Determine the values that you will specify for the following parameters:

Input Parameters for Gather Parameters for Rollback Patch from Home and Databases

Parameter Name	Default Value	Required	Description
Oracle Home	no default	required	Fully-qualified path name of the Oracle Home where the patch will be rolled back.
Oracle OS User	oracle	required	The OS user that owns the specified Oracle Home.
Patch Archive	no default	required	Name of the patch archive file. If the file does not exist on the target it will be downloaded from the software repository.

Additional Parameters Defined in this Step: Gather Advanced Parameters for Rollback Patch from Home and Databases v2

Parameter Name	Default Value	Required	Description
Cleanup	True	optional	Flag that determines whether any downloaded and extracted files will be cleaned up. Valid values are True and False.
Download Location	/tmp	optional	The directory on the target server where files are copied from the software repository—used only if the required files are not found on the target but are found in the software repository.

Additional Parameters Defined in this Step: Gather Advanced Parameters for Rollback Patch from Home and Databases v2, continued

Parameter Name	Default Value	Required	Description
Extract Location	/tmp	optional	Location where the archive files will be extracted.
Ignorable Oracle Errors	no default	optional	Comma-separated list of Oracle errors to be ignored when applying the patch to the database. This is in addition to the list of Oracle errors specified in the patch README. Values are of the form ORA-nnnnn. For example: ORA-04020,ORA-03113
OCM Response File	no default	optional	Path name of the Oracle Configuration Manager (OCM) response file. If not found on the target, this file is downloaded from the software repository. If left blank, a default response file will be created.
Oracle SIDs	ALL	optional	Oracle Instances (SIDs) that will be rolled back. Valid values are ALL, INCLUDE: followed by a comma-separated list of SIDs to be rolled back with the Oracle Home, and EXCLUDE: followed by a comma-separated list of Oracle SIDS to exclude from the rollback process.
Preparatory SQL Script	no default	optional	File name containing SQL statements that must be run before the database catalog update. This file is passed directly to SQLPlus and must be formatted as such. If it is not found on the target server, this file is downloaded from the software repository.
Rollback Current CPU Only	False	optional	Flag to specify only the molecule patches that are new to this CPU to be rolled back. Default value is False. This parameter is applicable only for CPU patch and Oracle 11g versions.
Run Database View Recompile	N	optional	Flag to indicate if the Database View Recompile step will be run.

Note: See ["Parameters for Oracle - Rollback Patch from Home and Databases"](#) on page 293 for detailed descriptions of all input parameters for this workflow, including default values.

3. In the workflow editor, expose any additional parameters that you need. You will specify values for those parameters when you create the deployment. You will specify values for those parameters when you create the deployment.
4. Save the changes to the workflow (click **Save** in the lower right corner).
5. Create a new deployment.

6. On the Parameters tab, specify values for the required parameters listed in step 2 and any additional parameters that you have exposed. You do not need to specify values for those parameters whose default values are appropriate for your environment.
7. On the Targets tab, specify one or more targets for this deployment.

Note: The targets need to be the same targets (servers) you used when you ran the Oracle - Patch Home and Database workflow.

8. Save the deployment (click **Save** in the lower right corner).
9. Run the workflow using this deployment.

To verify the results:

The workflow will complete and report SUCCESS on the Console if it has run successfully. If an error occurs during workflow execution, the error is logged, and the workflow terminates in the FAILURE state.

Optional: If you want to further verify that the patch was successfully removed from the Oracle Home:

1. Go to `$ORACLE_HOME/OPatch/opatch lsinventory -oh $ORACLE_HOME`
2. Check that the patch you rolled back is NOT on the list of patches.

Optional: If you want to further verify that the patch was successfully removed from the Oracle Database Instances associated with the Oracle Home:

1. Log in as an SQLPlus privileged user.
2. Set the ORACLE_HOME to your Oracle Home.
3. Run the command: **`$ORACLE_HOME/OPatch/opatch lsinventory`**
4. Verify that the patch number that you rolled back is NOT listed in the output.

Sample Scenario

It is very straightforward to run the ["Oracle - Rollback Patch from Home and Databases v2"](#) workflow. This topic shows you typical parameter values to use.

Input Parameters for Gather Parameters for Rollback Patch from Home and Databases v2

Parameter Name	Example Value	Description
Oracle Home	/u01/app/oracle/product/11.2.0/db1	Fully-qualified path name of the Oracle Home where the patch will be rolled back.
Oracle OS User	oracle	The OS user that owns the specified Oracle Home.
Patch Archive	p16902043_112030_Linux-x86-64.zip	Name of the patch archive file. If the file does not exist on the target it will be downloaded from the software repository.

Additional Parameters Defined in this Step: Gather Advanced Parameters for Rollback Patch from Home and Databases v2

Parameter Name	Example Value	Description
Cleanup	True	Flag that determines whether any downloaded and extracted files will be cleaned up. Valid values are True and False.
Download Location	/tmp	The directory on the target server where files are copied from the software repository—used only if the required files are not found on the target but are found in the software repository.
Extract Location	/tmp	Location where the archive files will be extracted.
Ignorable Oracle Errors	ORA-04020,ORA-03113	Comma-separated list of Oracle errors to be ignored when applying the patch to the database. This is in addition to the list of Oracle errors specified in the patch README. Values are of the form ORA-nnnnn.
OCM Response File	no default	Path name of the Oracle Configuration Manager (OCM) response file. If not found on the target, this file is downloaded from the software repository. If left blank, a default response file will be created.
Oracle SIDs	ALL	Oracle Instances (SIDs) that will be rolled back. Valid values are ALL, INCLUDE: followed by a comma-separated list of SIDs to be rolled back with the Oracle Home, and EXCLUDE: followed by a comma-separated list of Oracle SIDs to exclude from the rollback process.
Preparatory SQL Script		File name containing SQL statements that must be run before the database catalog update. This file is passed directly to SQLPlus and must be formatted as such. If it is not found on the target server, this file is downloaded from the software repository.
Rollback Current	False	Flag to specify only the molecule patches that are new to this CPU to be rolled back. Default value is False. This parameter is applicable only

Additional Parameters Defined in this Step: Gather Advanced Parameters for Rollback Patch from Home and Databases v2, continued

Parameter Name	Example Value	Description
CPU Only		for CPU patch and Oracle 11g versions.
Run Database View Recompile	N	Flag to indicate if the Database View Recompile step will be run.

Parameters for Oracle - Rollback Patch from Home and Databases

The following tables describe the required and optional input parameters for this workflow. For some parameters, if you do not specify a value for a parameter, a default value is assigned.

Only those parameters that are configurable in a standard deployment are listed here. Input parameters that must be mapped to output parameters of previous steps are not listed.

Input Parameters Defined in this Step: Gather Parameters for Rollback Patch from Home and Databases v2

Parameter Name	Default Value	Required	Description
Oracle Home	no default	required	Fully-qualified path name of the Oracle Home where the patch will be rolled back.
Oracle OS User	oracle	required	The OS user that owns the specified Oracle Home.
Patch Archive	no default	required	Name of the patch archive file. If the file does not exist on the target it will be downloaded from the software repository.

Additional Parameters Defined in this Step: Gather Advanced Parameters for Rollback Patch from Home and Databases v2

Parameter Name	Default Value	Required	Description
Cleanup	True	optional	Flag that determines whether any downloaded and extracted files will be cleaned up. Valid values are True and False.
Download Location	/tmp	optional	The directory on the target server where files are copied from the software repository—used only if the required files are not found on the target but are found in the software repository.
Extract Location	/tmp	optional	Location where the archive files will be extracted.
Ignorable Oracle Errors	no default	optional	Comma-separated list of Oracle errors to be ignored when applying the patch to the database. This is in addition to the list of Oracle errors specified in the patch README. Values are of the form ORA-nnnnn. For example: ORA-04020,ORA-03113
OCM Response File	no default	optional	Path name of the Oracle Configuration Manager (OCM) response file. If not found on the target, this file is downloaded from the software repository. If left blank, a default response file will be created.
Oracle SIDs	ALL	optional	Oracle Instances (SIDs) that will be rolled back. Valid values are ALL, INCLUDE: followed by a comma-separated list of SIDs to be rolled back with the Oracle Home, and EXCLUDE: followed by a comma-separated list of Oracle SIDs to exclude from the rollback process.
Preparatory SQL Script	no default	optional	File name containing SQL statements that must be run before the database catalog update. This file is passed directly to SQLPlus and must be formatted as such. If it is not found on

Additional Parameters Defined in this Step: Gather Advanced Parameters for Rollback Patch from Home and Databases v2, continued

Parameter Name	Default Value	Required	Description
			the target server, this file is downloaded from the software repository.
Rollback Current CPU Only	False	optional	Flag to specify only the molecule patches that are new to this CPU to be rolled back. Default value is False. This parameter is applicable only for CPU patch and Oracle 11g versions.
Run Database View Recompile	N	optional	Flag to indicate if the Database View Recompile step will be run.

Apply Oracle Patchset

This workflow applies an Oracle Software Patch Set to an existing Oracle Home and Oracle Database.

Before you can run the Apply Oracle Patchset workflow you must provide the Oracle Software Patch Set in one of the following forms:

- A software archive (ZIP or `cpio.gz` file) that exists on the software repository or the target machine
- Unarchived files on a CD, DVD, NFS mount, or similar device

For additional information about how the Apply Oracle Patchset workflow can be used with other provisioning and patching workflows see [How to Use the Workflows Together](#) topic.

Note the following:

- The Database Upgrade Assistant (DBUA) utility is not available in Oracle Database version 9.2.0 (and earlier).
- The workflow does not upgrade the following items:
 - Oracle Label Security
 - Oracle Data Vault
 - Oracle ASM
- The workflow does not run the `changePerm.sh` command.
- The workflow does not configure Oracle Configuration Manager (OCM) for a cloned home.
- The workflow does not update Database time zone definitions.

Caution: This workflow stops all processes running from the `ORACLE_HOME` in order to patch. This includes the Oracle Listener, which may be servicing Oracle Instances outside this `ORACLE_HOME`.

To use this workflow in your environment, see the following information:

Topic	Information Included
"Prerequisites for this Workflow"	List of prerequisites that must be satisfied before you can run this workflow
"How this Workflow Works"	Information about what the workflow does, including validation checks performed, steps executed, and a high-level process flow
"How to Run this Workflow"	Instructions for running this workflow in your environment
"Sample Scenario"	Examples of typical parameter values for this workflow
Parameters	List of input parameters for this workflow

Prerequisites for this Workflow

Be sure that the following prerequisites are satisfied before you run the ["Apply Oracle Patchset"](#) workflow:

- The latest DMA solution packs require the latest DMA platform. To use the latest solution packs, update the DMA platform. DMA 10.30 solution packs are supported on DMA 10.30 (and later).
- You have installed the DMA Database Patching Solution Pack.
- You need to have Oracle Database provisioned and operational. You can do this by running workflows found in the DMA Database Provisioning Solution Pack:

Oracle – Provision Database Software

Oracle – Provision Database

- You have an Oracle support contract and have downloaded the appropriate patches to software repository or to the target machine.
- You have read access to all specified inventory pointers (Linux/UNIX).

For more information about prerequisites for Oracle Database, refer to the [Oracle Product Documentation](#).

How this Workflow Works

The following information describes how the "Apply Oracle Patchset" workflow works:

Overview

This workflow does the following things in the order shown:

- The initial steps of the workflow prepare it to apply the Oracle Patch Set to the Oracle Home and Oracle Database. The workflow processes user input parameters, constructs commands used in subsequent steps, downloads any required files, uncompresses the archive files, and fetches the Oracle binaries and Instances.
- The workflow applies the Patch Set to the Oracle Home. The workflow updates the Oracle installer response file. Then it stops all processes using the Oracle Home. It runs platform-dependent steps. Then the workflow executes the Oracle Software Installer and completes the installation.
- The workflow configures the Oracle Database.
- The final steps of the workflow allow the workflow to end cleanly. The workflow stops and restarts all the Oracle processes. Then it cleans up the downloaded files.

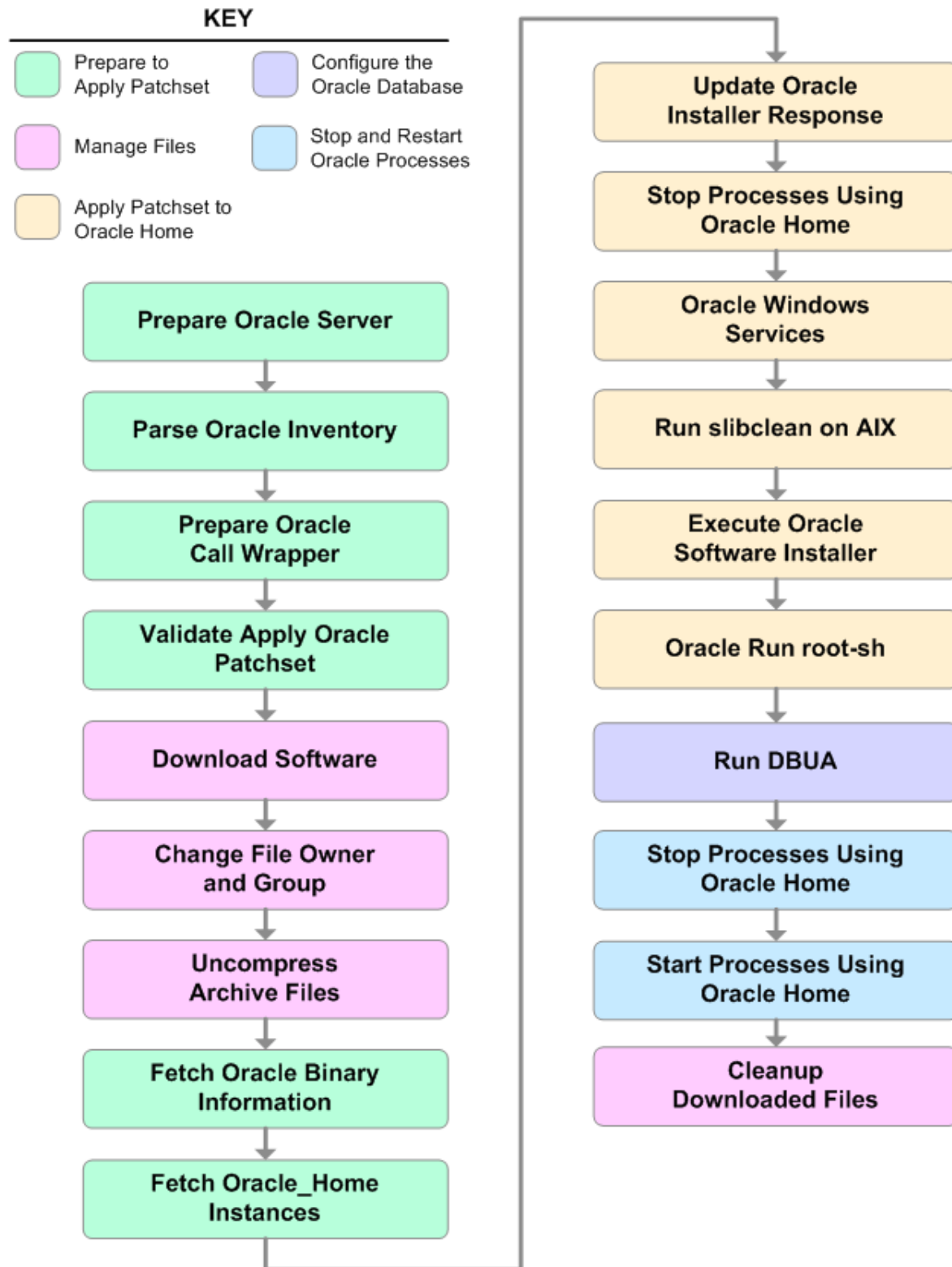
Validation Checks Performed

Much of the validation centers on the input parameters:

- The input parameters have the proper syntax (no special characters or spaces).
- Files exist or have valid specifications.

Steps Executed

The Apply Oracle Patchset workflow includes the following steps. Each step must complete successfully before the next step can start. If a step fails, the workflow reports a failure and all subsequent steps are skipped.



Steps Used in Apply Oracle Patchset

Workflow Step	Description
Prepare Oracle Server	This step prepares the target server for access by the OS administrative user.
Parse Oracle Inventory	<p>This step parses the specified Oracle inventory files (if they exist) and passes the inventory information to subsequent steps.</p> <ul style="list-style-type: none"> • If one or more Inventory Files are specified and they exist, the step parses these files and extracts their contents. • If no Inventory Files are specified, the step assigns the appropriate default and attempts to parse that file. • If one or more Inventory Files are specified and they do not exist, the step creates inventory information based on the specified Oracle Account and Oracle Home.
Prepare Oracle Call Wrapper	<p>This step constructs the commands needed to execute subsequent steps in the workflow as either the OS administrative user or the user who owns the pertinent ORACLE_HOME.</p> <p>The step also creates utility parameters that will be used by subsequent steps.</p>
Validate Apply Oracle Patchset	This step validates the values specified for the input parameters used by the "Apply Oracle Patchset" workflow. It also sets the values of various output parameters that will be consumed by subsequent steps.
Download Software	This step downloads a list of files to a specified location on the target server.
Change File Owner and Group	This step changes the ownership and group of each file specified. A warning is issued for files that are not found.
Uncompress Archive Files	For each supplied file, this step extracts the contents of the archive file (or files).
Fetch Oracle Binary Information	<p>This step fetches the fully qualified pathnames of the following files from the staging location in an Oracle software archive (either a Patch Set or the install software):</p> <pre>runInstaller products.xml rootpre.sh *.rsp.</pre>
Fetch Oracle Home Instances	This step fetches the list of Oracle Instances that share the specified ORACLE_HOME.
Update Oracle Installer Response	This step updates the provided installer response file or, if one is not provided, creates an installer response file based on a default response file provided by Oracle. This step is designed to be run by the owner of the ORACLE_HOME.

Steps Used in Apply Oracle Patchset, continued

Workflow Step	Description
Stop Processes Using Oracle Home	This step stops all Oracle Instances included in the Oracle SIDs list—excluding any specified in the Ignore SIDs list. The step attempts to stop the Oracle Agent.
Oracle Windows Services	This step preserves the list of Windows Services. This is necessary because the same step can be used more than once in a workflow.
Run slibclean on AIX	This step runs the <code>slibclean</code> command, if appropriate, on AIX targets.
Execute Oracle Software Installer	This step installs the Oracle software as defined by the response file. It is designed to be run as the Oracle software owner (typically oracle).
Oracle Run root-sh	This step runs the Oracle provided <code>root.sh</code> script in silent mode. It must be run as root.
Run DBUA	This step runs the Oracle Database Upgrade Assistant (DBUA) with the specified response file. It must be run as the Oracle software owner (typically oracle).
Stop Processes Using Oracle Home	This step stops all Oracle Instances included in the Oracle SIDs list—excluding any specified in the Ignore SIDs list. The step attempts to stop the Oracle Agent.
Start Processes Using Oracle Home	This step starts all Oracle Instances and Oracle Listeners in the Oracle SIDs list. It also attempts to start the Oracle Agent.
Cleanup Downloaded Files	This step removes all downloaded files and archives.

For parameter descriptions and defaults, see ["Parameters for Apply Oracle Patchset" on page 307](#).

How to Run this Workflow

The following instructions show you how to customize and run the ["Apply Oracle Patchset"](#) workflow in your environment.

Tip: For detailed instructions to run DMA workflows—using the Oracle - Compliance Audit workflow as an example—see DMA Quick Start Tutorial.

The workflow provides default values for some parameters. These default values are usually sufficient for a "typical" installation. You can override the defaults by specifying parameter values in the deployment. You can also expose additional parameters in the workflow, if necessary, to accomplish more advanced scenarios. Any parameters not explicitly specified in the deployment will have the default values listed in ["Parameters for Apply Oracle Patchset" on page 307](#)

Note: Before following this procedure, review the ["Prerequisites for this Workflow" on page 297](#), and ensure that all requirements are satisfied.

To run this workflow, you need to set your parameters differently depending on the location and status of your Oracle Patch Set. Use the following table to choose the method that matches your situation.

For information about uploading files to the DMA software repository, see [How to Import a File into the Software Repository on page 97](#).

To specify the Oracle Software Patch Set, choose one of the following methods:

Method 1: The Oracle ZIP file is in the software repository:

Note: The ZIP file must be downloaded from Oracle. Example: p6890831_111070_Linux-x86.zip.

1. In the Patchset Archive parameter, specify the name (or names) of the ZIP file (or files) that was downloaded from Oracle.
2. In the Download Location parameter, specify the directory where the ZIP file (or files) specified in the Patchset Archive parameter should be downloaded.
3. In the Software Archive Location parameter, specify the directory where the ZIP file (or files) specified in the Patchset Archive parameter should be extracted (unzipped).

All downloaded files are removed upon successful completion of the workflow.

Method 2: The Oracle ZIP file is stored on each target machine:

Note: The ZIP file must be downloaded from Oracle. Example: p6890831_111070_Linux-x86.zip.

1. In the Patchset Archive parameter, specify the fully qualified name (or names) of the ZIP file (or files) that was downloaded from Oracle.
2. You must specify a value for the Download Location parameter if the Install Response needs to be downloaded; otherwise, do not specify a value for Download Location.

All downloaded files are removed upon successful completion of the workflow.

To use the Apply Oracle Patchset workflow:

1. Create a deployable copy of the workflow.
2. Determine the values that you will specify for the following parameters:

Input Parameters for Parse Oracle Inventory

Parameter Name	Default Value	Required	Description
Inventory Files	see description	optional	Comma-separated list of fully-qualified Oracle inventory files. If not specified, set to the appropriate default value for the target server operating system. Defaults are: Solaris or HP-UX: /var/opt/oracle/oraInst.loc Linux: /etc/oraInst.loc
Oracle Home	no default	optional	Fully-qualified path name of the Oracle Home where the patch will be applied.

Input Parameters for Validate Apply Oracle Patchset

Parameter Name	Default Value	Required	Description
Download Location	/var/tmp	optional	The directory on the target server where files are copied from the software repository—used only if the required files are not found on the target but are found in the software repository.
Oracle Base	/u01/app/oracle	required	The location of the base directory for an Optimal Flexible Architecture (OFA) installation. This is typically called the ORACLE_BASE.
Patchset Archive	see description	required	Comma-separated list of relative or fully-qualified path names of the Oracle Patch Set archive files. If a fully-qualified path name points to a file, that file is expected to be on the target. If a relative path name points to a file, that file will be downloaded from the software directory on the DMA server. If a fully-qualified path name is a directory, the software is expected to be unzipped and ready to be applied. The default for UNIX targets is: /tmp/p5337014_10203_SOLARIS64.zip
Skip root-sh	N	optional	Skip running the rootpre.sh and root.sh scripts. Valid values are Y (yes) and N (no). Set to Y if an existing newer ORACLE_HOME is installed.
Software Archive	/var/tmp	optional	Directory location where the patch archives will be extracted.

Input Parameters for Update Oracle Installer Response

Parameter Name	Default Value	Required	Description
Install Edition	EE	optional	The product edition of the Oracle Database installation. Can be one of the following: SE (standard edition) or EE (enterprise edition).

Tip: To avoid having to re-enter passwords whenever they change, you can create a policy to provide them to the workflow (see [How to Use a Policy to Specify Parameter Values](#) on page 60).

Note: See ["Parameters for Apply Oracle Patchset" on page 307](#) for detailed descriptions of all input parameters for this workflow, including default values.

3. In the workflow editor, expose any additional parameters that you need. You will specify values for those parameters when you create the deployment.
4. Save the changes to the workflow (click **Save** in the lower right corner).
5. Create a new deployment.
6. On the Parameters tab, specify values for the required parameters listed in step 2 and any additional parameters that you have exposed. You do not need to specify values for those parameters whose default values are appropriate for your environment.
7. On the Targets tab, specify one or more targets for this deployment.
8. Save the deployment (click **Save** in the lower right corner).
9. Run the workflow using this deployment.

To verify the results:

The workflow will complete and report SUCCESS on the Console if it has run successfully. If an error occurs during workflow execution, the error is logged, and the workflow terminates in the FAILURE state.

Optional: If you want to further verify the results:

1. Log in to Oracle on the server where you deployed the Patch Set.
2. Check that the version that is running is the same as the deployed Patch Set, for example:

Oracle Database 11g 11.2.0.4.0

Sample Scenario

It is very straightforward to run the "Apply Oracle Patchset" workflow. This topic shows you typical parameter values to use.

Input Parameters for Parse Oracle Inventory

Parameter Name	Example Value	Description
Inventory Files	/etc/oraInst.loc	Comma-separated list of fully-qualified Oracle inventory files. If not specified, set to the appropriate default value for the target server operating system. Defaults are: Solaris or HP-UX: /var/opt/oracle/oraInst.loc Linux: /etc/oraInst.loc
Oracle Home	/u01/app/oracle/product/11.2.0/db1	Fully-qualified path name of the Oracle Home where the patch will be applied.

Input Parameters for Validate Apply Oracle Patchset

Parameter Name	Example Value	Description
Download Location	/var/tmp	The directory on the target server where files are copied from the software repository—used only if the required files are not found on the target but are found in the software repository.
Oracle Base	/u01/app/oracle	The location of the base directory for an Optimal Flexible Architecture (OFA) installation. This is typically called the ORACLE_BASE.
Patchset Archive	p5337014_10203_SOLARIS64.zip	Comma-separated list of relative or fully-qualified path names of the Oracle Patch Set archive files. If a fully-qualified path name points to a file, that file is expected to be on the target. If a relative path name points to a file, that file will be downloaded from the software directory on the DMA server. If a fully-qualified path name is a directory, the software is expected to be unzipped and ready to be applied. The default for UNIX targets is: /tmp/p5337014_10203_SOLARIS64.zip
Skip root-sh	N	Skip running the rootpre.sh and root.sh scripts. Valid values are Y (yes) and N (no). Set to Y if an existing newer ORACLE_HOME is installed.
Software Archive	/tmp/software	Directory location where the patch archives will be extracted.

Input Parameters for Update Oracle Installer Response

Parameter Name	Example Value	Description
Install Edition	EE	The product edition of the Oracle Database installation. Can be one of the following: SE (standard edition) or EE (enterprise edition).

Parameters for Apply Oracle Patchset

The following tables describe the required and optional input parameters for this workflow. Some of these parameters may not be initially visible in a deployment (see [How to Expose Additional Workflow Parameters](#) on page 93). For some parameters, if you do not specify a value for a parameter, a default value is assigned.

Note: Only those parameters that are configurable in a standard deployment are listed here. Input parameters that must be mapped to output parameters of previous steps are not listed.

Parameters Defined in this Step: Parse Oracle Inventory

Parameter Name	Default Value	Required	Description
Inventory Files	see description	optional	Comma-separated list of fully-qualified Oracle inventory files. If not specified, set to the appropriate default value for the target server operating system. Defaults are: Solaris or HP-UX: /var/opt/oracle/oraInst.loc Linux: /etc/oraInst.loc
Oracle Account	no default	optional	Oracle user who owns the ORACLE_HOME. Required if inventory does not exist.
Oracle Home	no default	optional	Fully-qualified path name of the Oracle Home where the patch will be applied.
Server Wrapper	see description	required	Command that will execute a step as the OS administrative user. The default for UNIX targets is: <code>sudo su - root /opt/hp/dma/client/jython.sh</code> Caution: This parameter is derived by the workflow. Under most circumstances, you should not change its mapping or its value.

Additional Parameters Defined in this Step: Validate Apply Oracle Patchset

Parameter Name	Default Value	Required	Description
Download Location	/var/tmp	optional	The directory on the target server where files are copied from the software repository—used only if the required files are not found on the target but are found in the software repository.
Ignore SIDs	no default	optional	Comma-separated list of Oracle Instances (SIDs) that should not be patched.
Install Response	no default	optional	Location of the Oracle Universal Installer response file.
Instance Wrapper	no default	required	Command that will be used to execute subsequent steps as the user who owns the ORACLE_HOME. For example: <code>su - oracle /opt/hp/dma/client/jython.sh</code>

Additional Parameters Defined in this Step: Validate Apply Oracle Patchset, continued

Parameter Name	Default Value	Required	Description
			Caution: This parameter is derived by the workflow. Under most circumstances, you should not change its mapping or its value.
Inventory Pointers	no default	optional	<p>Comma separated list of fully qualified inventory pathname directories.</p> <p>Caution: This parameter is derived by the workflow. Under most circumstances, you should not change its mapping or its value.</p>
Oracle Base	/u01/app/oracle	required	The location of the base directory for an Optimal Flexible Architecture (OFA) installation. This is typically called the ORACLE_BASE.
Oracle Home Info	no default	optional	<p>Dictionary list of all information discovered in the specified inventory file(s).</p> <p>Caution: This parameter is derived by the workflow. Under most circumstances, you should not change its mapping or its value.</p>
Patchset Archive	see description	required	<p>Comma-separated list of relative or fully-qualified path names of the Oracle Patch Set archive files.</p> <p>If a fully-qualified path name points to a file, that file is expected to be on the target. If a relative path name points to a file, that file will be downloaded from the software directory on the DMA server. If a fully-qualified path name is a directory, the software is expected to be unzipped and ready to be applied.</p> <p>The default for UNIX targets is: /tmp/p5337014_10203_SOLARIS64.zip</p>
Skip root-sh	N	optional	Skip running the rootpre.sh and root.sh scripts. Valid values are Y (yes) and N (no). Set to Y if an existing newer ORACLE_HOME is installed.
Software Archive	/var/tmp	optional	Directory location where the patch archives will be extracted.

Additional Parameters Defined in this Step: Update Oracle Installer Response

Parameter Name	Default Value	Required	Description
CRS Nodes	no default	optional	<p>List of all nodes where Oracle Clusterware is deployed.</p> <p>Caution: This parameter should only be specified for RAC and Cluster Ready systems.</p>
DBA Group	no default	optional	The DBA group to use for superuser access to the subsequent Oracle Database.

Additional Parameters Defined in this Step: Update Oracle Installer Response, continued

Parameter Name	Default Value	Required	Description
Install Edition	EE	optional	The product edition of the Oracle Database installation. Can be one of the following: SE (standard edition) or EE (enterprise edition).
Operator Group	no default	optional	The operator group to use for operator access to the subsequent Oracle Database.
Oracle Group	no default	optional	The Oracle software installation group. Caution: This parameter is derived by the workflow. Under most circumstances, you should not change its mapping or its value.
Oracle Home Name	no default	optional	The name of the ORACLE_HOME as recorded in the inventory. Caution: This parameter is derived by the workflow. Under most circumstances, you should not change its mapping or its value.
Oracle Products File	see description	optional	The fully qualified path name of the products.xml file. Default is: /tmp/Disk1/stage/products.xml Caution: This parameter is derived by the workflow. Under most circumstances, you should not change its mapping or its value.
Oracle Response Files	see description	optional	A comma-separated list of default response files. Default is: /tmp/Disk1/response/standard.rsp Caution: This parameter is derived by the workflow. Under most circumstances, you should not change its mapping or its value.
Oracle runInstaller	see description	optional	The fully qualified path name of the Oracle installer executable. Default is: /tmp/Disk1/runInstaller Caution: This parameter is derived by the workflow. Under most circumstances, you should not change its mapping or its value.
RAC One Node Install	false	optional	The oracle.install.db.isRACOneInstall option. If set to true, the installer will install Oracle RAC One Node software. Caution: This parameter should only be specified for RAC and Cluster Ready systems.
Temporary File Location	no default	optional	The location where all temporary output files will be placed. This directory will be removed at the completion of the workflow. Caution: This parameter is derived by the workflow.

Additional Parameters Defined in this Step: Update Oracle Installer Response, continued

Parameter Name	Default Value	Required	Description
			Under most circumstances, you should not change its mapping or its value.

Clone Oracle Home

This workflow makes a clone (copy) of an Oracle Home on the same server.

This workflow uses the tar facility to copy the Oracle Home. The new copy of the Oracle Home is then registered in the inventory using the Oracle Installer (`runInstaller`).

For additional information about how the Clone Oracle Home workflow can be used with other provisioning and patching workflows see [How to Use the Workflows Together](#) topic.

To use this workflow in your environment, see the following information:

Topic	Information Included
"Prerequisites for this Workflow"	List of prerequisites that must be satisfied before you can run this workflow
"How this Workflow Works"	Information about what the workflow does, including validation checks performed, steps executed, and a high-level process flow
"How to Run this Workflow"	Instructions for running this workflow in your environment
"Sample Scenario"	Examples of typical parameter values for this workflow
Parameters	List of input parameters for this workflow

Prerequisites for this Workflow

Be sure that the following prerequisites are satisfied before you run the ["Clone Oracle Home"](#) workflow:

- The latest DMA solution packs require the latest DMA platform. To use the latest solution packs, update the DMA platform. DMA10.50.001.000 solution packs are supported on DMA10.50.001.000 (and later).
- You have installed the DMA Database Patching Solution Pack .
- You need to have Oracle Database provisioned and operational. You can do this by running workflows found in the DMA Database Provisioning Solution Pack:

Oracle – Provision Database Software

Oracle – Provision Database

- You have an Oracle support contract and have downloaded the appropriate patches to the software repository or to the target machine.
- You have read access to all specified inventory pointers (Linux/UNIX).

For more information about prerequisites for Oracle Database, refer to the [Oracle Product Documentation](#).

How this Workflow Works

The following information describes how the "Clone Oracle Home" workflow works:

Overview

This workflow does the following things in the order shown:

- The initial steps of the workflow prepare it to clone the Oracle Home. The workflow processes user input parameters, and constructs commands used in subsequent steps.
- The workflow creates a clone (copy) of one or more specified Oracle Homes.

Validation Checks Performed

Much of the validation centers on the input parameters:

- The input parameters have the proper syntax (no special characters or spaces).
- Files exist or have valid specifications.

Steps Executed

The Clone Oracle Home workflow includes the following steps. Each step must complete successfully before the next step can start. If a step fails, the workflow reports a failure and all subsequent steps are skipped.

Steps Used in Clone Oracle Home

Workflow Step	Description
Prepare Server	This step prepares the Server Wrapper and Instance Wrapper, which enable subsequent steps to be executed by the OS administrator user or the owner of the database or middleware software.
Parse Oracle Inventory	<p>This step parses the specified Oracle inventory files (if they exist) and passes the inventory information to subsequent steps.</p> <ul style="list-style-type: none"> • If one or more Inventory Files are specified and they exist, the step parses these files and extracts their contents. • If no Inventory Files are specified, the step assigns the appropriate default and attempts to parse that file. • If one or more Inventory Files are specified and they do not exist, the step creates inventory information based on the specified Oracle Account and Oracle Home.
Prepare Oracle Call Wrapper	<p>This step constructs the commands needed to execute subsequent steps in the workflow as either the OS administrative user or the user who owns the pertinent ORACLE_HOME.</p> <p>The step also creates utility parameters that will be used by subsequent steps.</p>
Validate Clone Oracle Home	This step validates the values specified for the input parameters used by the "Clone Oracle Home" workflow. It also sets the values of various output parameters that will be consumed by subsequent steps.
Clone Oracle Homes	This step creates a copy of one or more specified Oracle homes.

For parameter descriptions and defaults, see ["Parameters for Clone Oracle Home" on page 318](#).

How to Run this Workflow

The following instructions show you how to customize and run the ["Clone Oracle Home"](#) workflow in your environment.

The workflow provides default values for some parameters. These default values are usually sufficient for a "typical" installation. You can override the defaults by specifying parameter values in the deployment. You can also expose additional parameters in the workflow, if necessary, to accomplish more advanced scenarios. Any parameters not explicitly specified in the deployment will have the default values listed in ["Parameters for Clone Oracle Home" on page 318](#).

Note: Before following this procedure, review the ["Prerequisites for this Workflow" on page 312](#) and ensure that all requirements are satisfied.

To use the Clone Oracle Home workflow:

1. Create a deployable copy of the workflow.
2. Determine the values that you will specify for the following parameters:

Input Parameters for Parse Oracle Inventory

Parameter Name	Default Value	Required	Description
Inventory Files	see description	optional	Comma-separated list of fully-qualified Oracle inventory files. If not specified, set to the appropriate default value for the target server operating system. Defaults are: Solaris or HP-UX: /var/opt/oracle/oraInst.loc Linux: /etc/oraInst.loc

Input Parameters for Validate Clone Oracle Home

Parameter Name	Default Value	Required	Description
New Oracle Homes	see description	optional	Comma-separated list of the Oracle homes (fully qualified paths) that will be cloned (copied) from the Oracle Homes list. There must be one New Oracle Home for each Clone Oracle Home. Default is: /u01/app/oracle/product/11.2.0.0/DB4
Oracle Homes	see description	optional	Comma-separated list of Oracle Homes (fully qualified path names) that will be cloned. One or more is required. Default is: /u01/app/oracle/product/11.2.0.0/DB2

Tip: To avoid having to re-enter passwords whenever they change, you can create a policy to provide them to the workflow.

Note: See ["Parameters for Clone Oracle Home" on page 318](#) for detailed descriptions of all input parameters for this workflow, including default values.

3. In the workflow editor, expose any additional parameters that you need. You will specify values for those parameters when you create the deployment.
4. Save the changes to the workflow (click **Save** in the lower right corner).
5. Create a new deployment.
6. On the Parameters tab, specify values for the required parameters listed in step 2 and any additional parameters that you have exposed. You do not need to specify values for those parameters whose default values are appropriate for your environment.
7. On the Targets tab, specify one or more targets for this deployment.
8. Save the deployment (click **Save** in the lower right corner).
9. Run the workflow using this deployment.

To verify the results:

The workflow will complete and report SUCCESS on the Console if it has run successfully. If an error occurs during workflow execution, the error is logged, and the workflow terminates in the FAILURE state.

Optional: If you want to further verify the results:

1. Go to the location where the Oracle Home was cloned.
2. Check that your important folders and files were created.

Sample Scenario

It is very straightforward to run the "Clone Oracle Home" workflow. This topic shows you typical parameter values to use.

Input Parameters for Parse Oracle Inventory

Parameter Name	Example Value	Description
Inventory Files	/etc/oraInst.loc	Comma-separated list of fully-qualified Oracle inventory files. If not specified, set to the appropriate default value for the target server operating system. Defaults are: Solaris or HP-UX: /var/opt/oracle/oraInst.loc Linux: /etc/oraInst.loc

Input Parameters for Validate Clone Oracle Home

Parameter Name	Example Value	Description
New Oracle Homes	/opt/app/oracle/product/11.2.0/DB4	Comma-separated list of the Oracle homes (fully qualified paths) that will be cloned (copied) from the Oracle Homes list. There must be one New Oracle Home for each Clone Oracle Home. Default is: /u01/app/oracle/product/11.2.0.0/DB4
Oracle Homes	/opt/app/oracle/product/11.2.0/DB2	Comma-separated list of Oracle Homes (fully qualified path names) that will be cloned. One or more is required. Default is: /u01/app/oracle/product/11.2.0.0/DB2

Parameters for Clone Oracle Home

The following tables describe the required and optional input parameters for this workflow. Some of these parameters may not be initially visible in a deployment. For some parameters, if you do not specify a value for a parameter, a default value is assigned.

Note: Only those parameters that are configurable in a standard deployment are listed here. Input parameters that must be mapped to output parameters of previous steps are not listed.

Parameters Defined in this Step: Parse Oracle Inventory

Parameter Name	Default Value	Required	Description
Inventory Files	see description	optional	Comma-separated list of fully-qualified Oracle inventory files. If not specified, set to the appropriate default value for the target server operating system. Defaults are: Solaris or HP-UX: /var/opt/oracle/oraInst.loc Linux: /etc/oraInst.loc
Oracle Account	no default	optional	Oracle user who owns the ORACLE_HOME. Required if inventory does not exist.
Oracle Home	no default	optional	Fully-qualified path name of the Oracle Home where the patch will be applied.
Server Wrapper	see description	required	Command that will execute a step as the OS administrative user. The default for UNIX targets is: <code>sudo su - root /opt/hp/dma/client/jython.sh</code> This parameter is derived by the workflow. Under most circumstances, you should not change its mapping or its value.

Additional Parameters Defined in this Step: Validate Clone Oracle Home

Parameter Name	Default Value	Required	Description
Instance Wrapper	no default	required	Command that will be used to execute subsequent steps as the user who owns the ORACLE_HOME. For example: <code>su - oracle /opt/hp/dma/client/jython.sh</code> Caution: This parameter is derived by the workflow. Under most circumstances, you should not change its mapping or its value.
New Oracle Home Names	Ora102A	optional	Comma-separated list of Oracle Home Names for the cloned Oracle homes. There must be one New Oracle Home Name for each New Oracle Home.
New Oracle Homes	see description	optional	Comma-separated list of the Oracle homes (fully qualified paths) that will be cloned (copied) from the Oracle Homes list. There must be one New Oracle Home for each Clone Oracle

Additional Parameters Defined in this Step: Validate Clone Oracle Home , continued

Parameter Name	Default Value	Required	Description
			Home. Default is: /u01/app/oracle/product/11.2.0.0/DB4
Oracle Homes	see description	optional	Comma-separated list of Oracle Homes (fully qualified path names) that will be cloned. One or more is required. Default is: /u01/app/oracle/product/11.2.0.0/DB2
Oracle Inventory Info	no default	optional	Dictionary list of all information discovered in the supplied inventory file(s).

Migrate Oracle Home

This workflow moves an Oracle Instance from one Oracle Home to another Oracle Home.

For additional information about how the Migrate Oracle Home workflow can be used with other patching workflows see [How to Use the Workflows Together](#) topic.

To use this workflow in your environment, see the following information:

Topic	Information Included
Prerequisites for this Workflow	List of prerequisites that must be satisfied before you can run this workflow
How this Workflow Works	Information about what the workflow does, including validation checks performed, steps executed, and a high-level process flow
How to Run this Workflow	Instructions for running this workflow in your environment
Sample Scenario	Examples of typical parameter values for this workflow
Parameters	List of input parameters for this workflow

Prerequisites for this Workflow

Be sure that the following prerequisites are satisfied before you run the ["Migrate Oracle Home"](#) workflow:

- The latest DMA solution packs require the latest DMA platform. To use the latest solution packs, update the DMA platform. DMA10.50.001.000 solution packs are supported on DMA10.50.001.000 (and later).
- You have installed the DMA Database Patching Solution Pack .
- You need to have Oracle Database provisioned and operational. You can do this by running workflows found in the DMA Database Provisioning Solution Pack:

Oracle – Provision Database Software

Oracle – Provision Database
- You have an Oracle support contract and have downloaded the appropriate patches to software repository or to the target machine.
- You have read access to all specified inventory pointers (Linux/UNIX).

For more information about prerequisites for Oracle Database, refer to the [Oracle Product Documentation](#).

How this Workflow Works

The following information describes how the "Migrate Oracle Home" workflow works:

Overview

This workflow does the following things in the order shown:

- The initial steps of the workflow prepare it to move an Oracle Instance from one Oracle Home to another Oracle Home. The workflow prepares the server, determines the Oracle Home, parses the Oracle inventory, constructs commands used in subsequent steps, and processes user input parameters,
- The workflow migrates the Oracle Instance. The workflow shuts down the Oracle Instances, Oracle Listeners, and the Oracle Agent. It copies the Oracle configuration files and the Oracle network files. It resets the Oracle Home in the network files.
- The final steps of the workflow allow the workflow to end cleanly. The workflow restarts all the Oracle Instances, all Oracle Listeners, and the Oracle Agent. Then it shuts down these processes and restarts them to force a clean run environment. Then it associates the Oracle Instance with the Oracle Home in the `oratab` file.

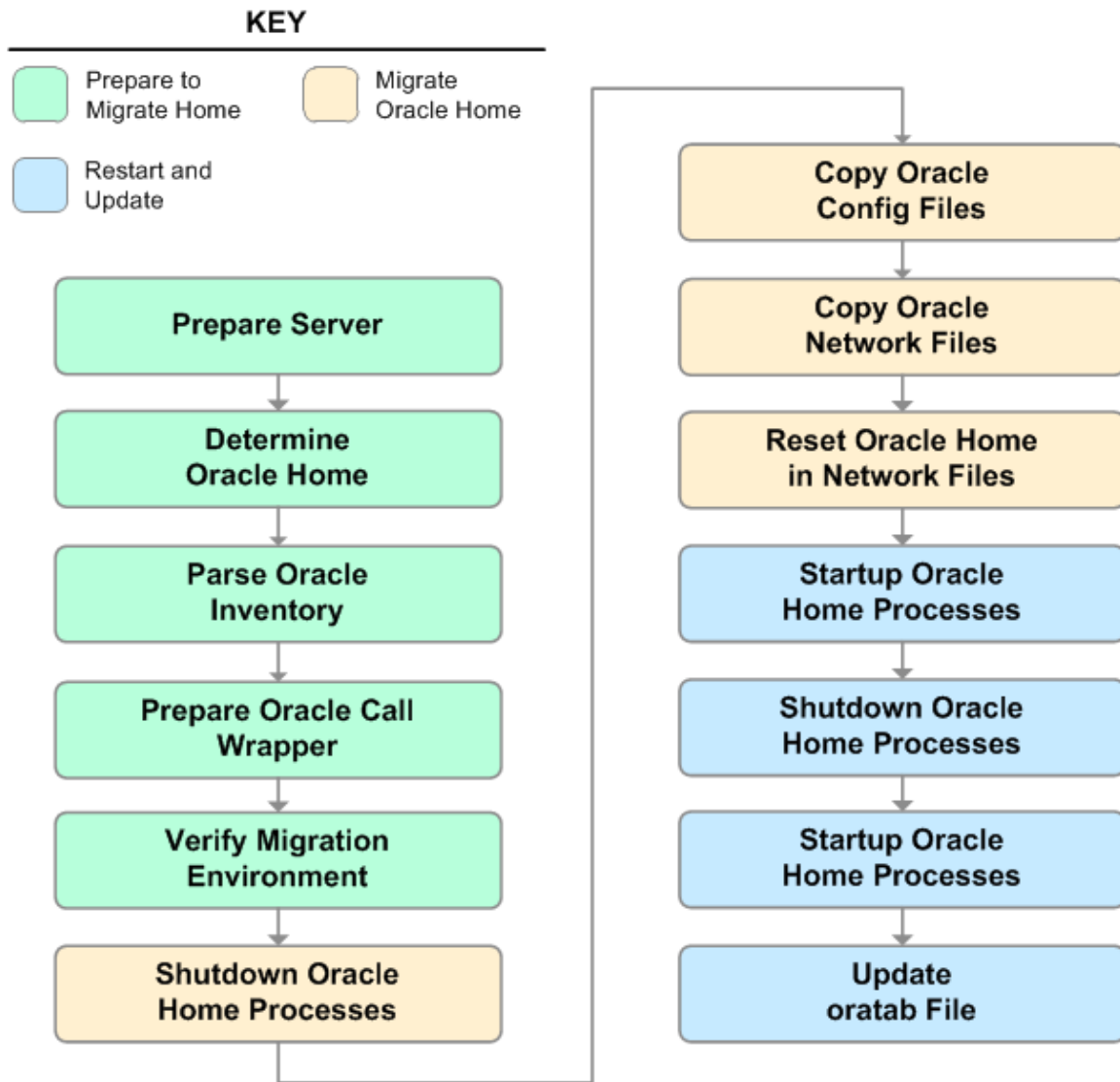
Validation Checks Performed

Much of the validation centers on the input parameters:

- The directories specified in the Current Oracle Home, New Oracle Home, Oracle SIDS, and Listeners parameters exist on the target.
- There are entries in the `oratab` file for the specified Oracle SIDs.
- There are entries in the `listener.ora` file for the specified Oracle Listeners.

Steps Executed

The Migrate Oracle Home workflow includes the following steps. Each step must complete successfully before the next step can start. If a step fails, the workflow reports a failure and all subsequent steps are skipped.



Steps Used in Migrate Oracle Home

Workflow Step	Description
Prepare Server	This step prepares the Server Wrapper and Instance Wrapper, which enable subsequent steps to be executed by the OS administrator user or the owner of the database or middleware software.
Determine Oracle Home	This step determines the value of ORACLE_HOME from the <code>/etc/oratab</code> or <code>/var/opt/oracle/oratab</code> file on UNIX targets.
Parse Oracle Inventory	<p>This step parses the specified Oracle inventory files (if they exist) and passes the inventory information to subsequent steps.</p> <ul style="list-style-type: none"> • If one or more Inventory Files are specified and they exist, the step parses these files and extracts their contents. • If no Inventory Files are specified, the step assigns the appropriate default and attempts to parse that file. • If one or more Inventory Files are specified and they do not exist, the step creates inventory information based on the specified Oracle Account and Oracle Home.
Prepare Oracle Call Wrapper	<p>This step constructs the commands needed to execute subsequent steps in the workflow as either the OS administrative user or the user who owns the pertinent ORACLE_HOME.</p> <p>The step also creates utility parameters that will be used by subsequent steps.</p>
Verify Migration Environment	<p>This step verifies the input parameters used throughout the Migrate Oracle Home workflow:</p> <ul style="list-style-type: none"> • The directories specified in the Current Oracle Home, New Oracle Home, Oracle SIDS, and Listeners parameters exist on the target. • There are entries in the <code>oratab</code> file for the specified Oracle SIDs. • There are entries in the <code>listener.ora</code> file for the specified Oracle Listeners.
Shutdown Oracle Home Processes	This step stops the Oracle Instances specified in the Oracle SIDs list—excluding those Oracle Instances in the Ignore SIDs list. It also stops all Oracle Listeners in the Listeners list and attempts to stop the Oracle Agent.
Copy Oracle Config Files	This step copies the Oracle configuration files from the current (source) Oracle home to the new (destination) Oracle home.
Copy Oracle Network Files	<p>This step copies the following files from the <code>\${Current Oracle Home}/network/admin</code> directory to the <code>\${New Oracle Home}/network/admin</code> directory:</p> <ul style="list-style-type: none"> • <code>tnsnames.ora</code> • <code>listener.ora</code> • <code>sqlnet.ora</code>
Reset Oracle Home in Network Files	This step resets the ORACLE_HOME value in the <code>\${New Oracle Home}/network/admin</code> files to reflect the <code>\${New Oracle Home}</code> value.

Steps Used in Migrate Oracle Home, continued

Workflow Step	Description
Startup Oracle Home Processes	This step starts the Oracle Instances specified in the Oracle SIDs list—excluding those Oracle Instances in the Ignore SIDs list. It also starts all Oracle Listeners in the Listeners list and attempts to start the Oracle Agent.
Shutdown Oracle Home Processes	This step stops the Oracle Instances specified in the Oracle SIDs list—excluding those Oracle Instances in the Ignore SIDs list. It also stops all Oracle Listeners in the Listeners list and attempts to stop the Oracle Agent.
Startup Oracle Home Processes	This step starts the Oracle Instances specified in the Oracle SIDs list—excluding those Oracle Instances in the Ignore SIDs list. It also starts all Oracle Listeners in the Listeners list and attempts to start the Oracle Agent.
Update oratab File	This step updates the \${oratab directory}/oratab file that associates the ORACLE_SID and ORACLE_HOME values. It replaces entries with the \${Current Oracle Home} value with the \${New Oracle Home} value.

For parameter descriptions and defaults, see ["Parameters for Migrate Oracle Home" on page 330](#).

How to Run this Workflow

The following instructions show you how to customize and run the ["Migrate Oracle Home"](#) workflow in your environment.

Tip: For detailed instructions to run DMA workflows—using the Oracle - Compliance Audit workflow as an example—see *Quick Start Tutorial*.

The workflow provides default values for some parameters. These default values are usually sufficient for a "typical" installation. You can override the defaults by specifying parameter values in the deployment. You can also expose additional parameters in the workflow, if necessary, to accomplish more advanced scenarios. Any parameters not explicitly specified in the deployment will have the default values listed in ["Parameters for Migrate Oracle Home" on page 330](#).

Note: Before following this procedure, review the ["Prerequisites for this Workflow" on page 321](#), and ensure that all requirements are satisfied.

To use the Migrate Oracle Home workflow:

1. Create a deployable copy of the workflow.
2. Determine the values that you will specify for the following parameters:

Input Parameters for Parse Oracle Inventory

Parameter Name	Default Value	Required	Description
Inventory Files	see description	optional	Comma-separated list of fully-qualified Oracle inventory files. If not specified, set to the appropriate default value for the target server operating system. Defaults are: Solaris or HP-UX: /var/opt/oracle/oraInst.loc Linux: /etc/oraInst.loc

Input Parameters for Verify Migration Environment

Parameter Name	Default Value	Required	Description
Listeners	no default	optional	Comma-separated list of the Oracle Listener names to be included in start-up and shut-down sequences.
New Oracle Home	no default	required	File system location of the new ORACLE_HOME (migration destination).

Tip: To avoid having to re-enter passwords whenever they change, you can create a policy to provide them to the workflow.

Note: See ["Parameters for Migrate Oracle Home" on page 330](#) for detailed descriptions of all

input parameters for this workflow, including default values.

3. In the workflow editor, expose any additional parameters that you need . You will specify values for those parameters when you create the deployment.
4. Save the changes to the workflow (click **Save** in the lower right corner).
5. Create a new deployment.
6. On the Parameters tab, specify values for the required parameters listed in step 2 and any additional parameters that you have exposed. You do not need to specify values for those parameters whose default values are appropriate for your environment.
7. On the Targets tab, specify one or more targets for this deployment.
8. Save the deployment (click **Save** in the lower right corner).
9. Run the workflow using this deployment.

To verify the results:

The workflow will complete and report SUCCESS on the Console if it has run successfully. If an error occurs during workflow execution, the error is logged, and the workflow terminates in the FAILURE state.

Optional: If you want to further verify the results:

Make sure that you can log in to the server where your Oracle Database was migrated.

Sample Scenario

The following use cases demonstrate different ways that the "Migrate Oracle Home" workflow can be run:

Scenario 1: To migrate Oracle Home without shutting down and starting up the Listeners

For this use case, you leave the Listeners parameter blank.

Input Parameters for Parse Oracle Inventory

Parameter Name	Example Value	Description
Inventory Files	/etc/oraInst.loc	Comma-separated list of fully-qualified Oracle inventory files. If not specified, set to the appropriate default value for the target server operating system. Defaults are: Solaris or HP-UX: /var/opt/oracle/oraInst.loc Linux: /etc/oraInst.loc

Input Parameters for Verify Migration Environment

Parameter Name	Example Value	Description
Listeners		Comma-separated list of the Oracle Listener names to be included in start-up and shut-down sequences.
New Oracle Home	/u01/app/oracle/product/11.2.0/db4	File system location of the new ORACLE_HOME (migration destination).

Scenario 2: To migrate Oracle Home with shutting down and starting up the Listeners

For this use case, you set the Listeners parameter to a comma-separated list of Oracle Listener names.

Input Parameters for Parse Oracle Inventory

Parameter Name	Example Value	Description
Inventory Files	/etc/oraInst.loc	Comma-separated list of fully-qualified Oracle inventory files. If not specified, set to the appropriate default value for the target server operating system. Defaults are: Solaris or HP-UX: /var/opt/oracle/oraInst.loc Linux: /etc/oraInst.loc

Input Parameters for Verify Migration Environment

Parameter Name	Example Value	Description
Listeners	LISTENER1, LISTENER2	Comma-separated list of the Oracle Listener names to be included in start-up and shut-down sequences.
New Oracle Home	/u01/app/oracle/product/11.2.0/db4	File system location of the new ORACLE_HOME (migration destination).

Parameters for Migrate Oracle Home

The following tables describe the required and optional input parameters for this workflow. Some of these parameters may not be initially visible in a deployment. For some parameters, if you do not specify a value for a parameter, a default value is assigned.

Note: Only those parameters that are configurable in a standard deployment are listed here. Input parameters that must be mapped to output parameters of previous steps are not listed.

Parameters Defined in this Step: Parse Oracle Inventory

Parameter Name	Default Value	Required	Description
Inventory Files	see description	optional	Comma-separated list of fully-qualified Oracle inventory files. If not specified, set to the appropriate default value for the target server operating system. Defaults are: Solaris or HP-UX: /var/opt/oracle/oraInst.loc Linux: /etc/oraInst.loc
Oracle Account	no default	optional	Oracle user who owns the ORACLE_HOME. Required if inventory does not exist.
Oracle Home	no default	optional	Fully-qualified path name of the Oracle Home where the patch will be applied. Caution: This parameter is derived by the workflow. Under most circumstances, you should not change its mapping or its value.
Server Wrapper	see description	required	Command that will execute a step as the OS administrative user. The default for UNIX targets is: sudo su - root /opt/hp/dma/client/jython.sh Caution: This parameter is derived by the workflow. Under most circumstances, you should not change its mapping or its value.

Additional Parameters Defined in this Step: Verify Migration Environment

Parameter Name	Default Value	Required	Description
Call Wrapper	no default	required	Command used to execute a step as the Oracle Instance owner. For example: sudo -u oracle /opt/hp/dma/client/jython.sh Caution: This parameter is derived by the workflow. Under most circumstances, you should not change its mapping or its value.
Current Oracle Home	no default	required	File system location of the existing ORACLE_HOME (migration source).

Additional Parameters Defined in this Step: Verify Migration Environment, continued

Parameter Name	Default Value	Required	Description
			Caution: This parameter is derived by the workflow. Under most circumstances, you should not change its mapping or its value.
Listeners	no default	optional	Comma-separated list of the Oracle Listener names to be included in start-up and shut-down sequences.
New Oracle Home	no default	required	File system location of the new ORACLE_HOME (migration destination).
Oracle SIDs	no default	optional	Comma-separated list of the Oracle Instances (ORACLE_SIDs) in this ORACLE_HOME where the step's action should be performed. Caution: This parameter is derived by the workflow. Under most circumstances, you should not change its mapping or its value.

Additional Parameters Defined in this Step: Shutdown Oracle Home Processes

Parameter Name	Default Value	Required	Description
Ignore SIDs	TST,DEV	optional	Comma-separated list of Oracle Instances (SIDs) that should not be patched.

Oracle - Migrate and Patch Grid Managed Database

This workflow is designed to migrate and patch a database to a new home. The database is managed by Oracle Grid Infrastructure. The workflow will work for both Grid Standalone and Grid Cluster environments. The workflow is a database level workflow so you can migrate each database individually..

For additional information about how the Oracle - Migrate and Patch Grid Managed Database workflow can be used with other patching workflows see [How to Use the Workflows Together](#) topic.

To use this workflow in your environment, see the following information:

Topic	Information Included
"Prerequisites for this Workflow" on the next page	List of prerequisites that must be satisfied before you can run this workflow
"How this Workflow Works" on page 334	Information about what the workflow does, including validation checks performed, steps executed, and a high-level process flow
"How to Run this Workflow" on page 336	Instructions for running this workflow in your environment
"Parameters for Oracle - Migrate and Patch Grid Managed Database" on page 339	List of input parameters for this workflow

Prerequisites for this Workflow

Be sure that the following prerequisites are satisfied before you run the Oracle - Migrate and Patch Grid Managed Database workflow:

- The latest DMA solution packs require the latest DMA platform. To use the latest solution packs, update the DMA platform. DMA10.50.001.000 solution packs are supported on DMA10.50.001.000 (and later).
- You have installed the DMA Database Patching Solution Pack .
- You need to have Oracle Database provisioned and operational. You can do this by running workflows found in the DMA Database Provisioning Solution Pack:

Oracle – Provision Database Software

Oracle – Provision Database
- You have an Oracle support contract and have downloaded the appropriate patches to software repository or to the target machine.
- You have read access to all specified inventory pointers (Linux/UNIX).

For more information about prerequisites for Oracle Database, refer to the [Oracle Product Documentation](#).

How this Workflow Works

The following information describes how the Oracle - Migrate and Patch Grid Managed Database workflow works:

Overview

This workflow does the following things in the order shown:

- The initial steps of the workflow prepare it to move an Oracle Instance from one Oracle Home to another Oracle Home. The workflow prepares the server, determines the Oracle Home, parses the Oracle inventory, constructs commands used in subsequent steps, and processes user input parameters,
- The workflow migrates the Oracle Instance. The workflow shuts down the Oracle Instances, Oracle Listeners, and the Oracle Agent. It copies the Oracle configuration files and the Oracle network files. It resets the Oracle Home in the network files.
- The final steps of the workflow allow the workflow to end cleanly. The workflow restarts all the Oracle Instances, all Oracle Listeners, and the Oracle Agent. Then it shuts down these processes and restarts them to force a clean run environment. Then it associates the Oracle Instance with the Oracle Home in the `oratab` file.

Validation Checks Performed

Much of the validation centers on the input parameters:

- The directories specified in the Current Oracle Home, New Oracle Home, Oracle SIDS, and Listeners parameters exist on the target.
- There are entries in the `oratab` file for the specified Oracle SIDs.
- There are entries in the `listener.ora` file for the specified Oracle Listeners.

Steps Executed

The Oracle - Migrate and Patch Grid Managed Database workflow includes the following steps. Each step must complete successfully before the next step can start. If a step fails, the workflow reports a failure and all subsequent steps are skipped.

Steps Used in Oracle - Migrate and Patch Grid Managed Database

Workflow Step	Description
Gather Parameters for Migrate and Patch Grid Managed Database	This step gathers the required parameters for Migrate and Patch Grid Managed Database.
Migrate and Patch Database	This step migrates the Oracle instance to a new home and patches the database.

For parameter descriptions and defaults, see [Parameters for Oracle - Migrate and Patch Grid Managed Database](#).

How to Run this Workflow

The following instructions show you how to customize and run the Oracle - Migrate and Patch Grid Managed Database workflow in your environment.

Tip: For detailed instructions to run DMA workflows—using the Oracle - Compliance Audit workflow as an example—see *Quick Start Tutorial*.

The workflow provides default values for some parameters. These default values are usually sufficient for a "typical" installation. You can override the defaults by specifying parameter values in the deployment. You can also expose additional parameters in the workflow, if necessary, to accomplish more advanced scenarios. Any parameters not explicitly specified in the deployment will have the default values listed in Parameters for Oracle - Migrate and Patch Grid Managed Database.

Note: Before following this procedure, review the Prerequisites for this Workflow, and ensure that all requirements are satisfied.

To use the Oracle - Migrate and Patch Grid Managed Database workflow:

1. Create a deployable copy of the workflow.
2. Determine the values that you will specify for the following parameters:

Input Parameters for Gather Parameters for Migrate and Patch Grid Managed Database

Parameter Name	Default Value	Required	Description
Ignorable Oracle Errors	no default	optional	Comma-separated list of Oracle errors to be ignored when applying the patch to the database. This is in addition to the list of Oracle errors specified in the patch readme. Values are of the form ORA-nnnnn. Example: ORA-04020,ORA-03113
New Oracle Home	no default	optional	File system location of the new ORACLE_HOME (migration destination).
Oracle OS User	oracle	required	The OS user that owns the specified Oracle Home.

Input Parameters for Migrate and Patch Grid Managed Database

Parameter Name	Default Value	Required	Description
Call Wrapper	no default	required	<p>Command used to execute a step as the Oracle Instance owner. For example:</p> <pre>sudo -u oracle /opt/hp/dma/client/jython.sh</pre> <p>Caution: This parameter is derived by the workflow. Under most circumstances, you should</p>

Input Parameters for Migrate and Patch Grid Managed Database, continued

Parameter Name	Default Value	Required	Description
			<p>not change its mapping or its value.</p> <p>Caution: This parameter is derived by the workflow. Under most circumstances, you should not change its mapping or its value.</p>
Database Name	no default	required	The name of the new database.
Grid Nodes	no default	optional	Comma separated list of nodes that are part of a Grid Infrastructure environment. By default, the nodes are discovered by olsnodes and then all nodes are rolled back.
Ignorable Oracle Errors	no default	optional	Comma-separated list of Oracle errors to be ignored when applying the patch to the database. This is in addition to the list of Oracle errors specified in the patch readme. Values are of the form ORA-nnnnn. Example: ORA-04020,ORA-03113
Instance Name	no default	Required	The Oracle Database Instance Name.
New Oracle Home	no default	required	File system location of the new ORACLE_HOME (migration destination).
Oracle Home	no default	required	File system location of the current ORACLE_HOME.
Oracle OS User	oracle	required	The OS user that owns the specified Oracle Home.
Oracle Version	no default	optional	Version of the Oracle Installation

Tip: To avoid having to re-enter passwords whenever they change, you can create a policy to provide them to the workflow.

Note: See Parameters for Oracle - Migrate and Patch Grid Managed Database for detailed descriptions of all input parameters for this workflow, including default values.

3. In the workflow editor, expose any additional parameters that you need . You will specify values for those parameters when you create the deployment.
4. Save the changes to the workflow (click **Save** in the lower right corner).
5. Create a new deployment.

6. On the Parameters tab, specify values for the required parameters listed in step 2 and any additional parameters that you have exposed. You do not need to specify values for those parameters whose default values are appropriate for your environment.
7. On the Targets tab, specify one or more targets for this deployment.
8. Save the deployment (click **Save** in the lower right corner).
9. Run the workflow using this deployment.

To verify the results:

The workflow will complete and report SUCCESS on the Console if it has run successfully. If an error occurs during workflow execution, the error is logged, and the workflow terminates in the FAILURE state.

Optional: If you want to further verify the results:

Make sure that you can log in to the server where your Oracle Database was migrated.

Parameters for Oracle - Migrate and Patch Grid Managed Database

The following tables describe the required and optional input parameters for this workflow. Some of these parameters may not be initially visible in a deployment. For some parameters, if you do not specify a value for a parameter, a default value is assigned.

Note: Only those parameters that are configurable in a standard deployment are listed here. Input parameters that must be mapped to output parameters of previous steps are not listed.

Parameters Defined in this Step: Gather Parameters for Migrate and Patch Grid Managed Database

Parameter Name	Default Value	Required	Description
Ignorable Oracle Errors	no default	optional	Comma-separated list of Oracle errors to be ignored when applying the patch to the database. This is in addition to the list of Oracle errors specified in the patch readme. Values are of the form ORA-nnnnn. Example: ORA-04020,ORA-03113
New Oracle Home	no default	optional	File system location of the new ORACLE_HOME (migration destination).
Oracle OS User	oracle	required	The OS user that owns the specified Oracle Home.
Ignorable Oracle Errors	no default	optional	Comma-separated list of Oracle errors to be ignored when applying the patch to the database. This is in addition to the list of Oracle errors specified in the patch readme. Values are of the form ORA-nnnnn. Example: ORA-04020,ORA-03113

Additional Parameters Defined in this Step: Migrate and Patch Grid Managed Database

Parameter Name	Default Value	Required	Description
Call Wrapper	no default	required	<p>Command used to execute a step as the Oracle Instance owner. For example:</p> <pre>sudo -u oracle /opt/hp/dma/client/jython.sh</pre> <p>Caution: This parameter is derived by the workflow. Under most circumstances, you should not change its mapping or its value.</p> <p>Caution: This parameter is derived by the workflow. Under most circumstances, you should not change its mapping or its value.</p>
Database Name	no default	required	The name of the new database.
Grid Nodes	no default	optional	Comma separated list of nodes that are part of a Grid Infrastructure environment. By default, the nodes are discovered by olsnodes and then all nodes are rolled back.

Additional Parameters Defined in this Step: Migrate and Patch Grid Managed Database, continued

Parameter Name	Default Value	Required	Description
Ignorable Oracle Errors	no default	optional	Comma-separated list of Oracle errors to be ignored when applying the patch to the database. This is in addition to the list of Oracle errors specified in the patch readme. Values are of the form ORA-nnnnn. Example: ORA-04020,ORA-03113
Instance Name	no default	Required	The Oracle Database Instance Name.
New Oracle Home	no default	required	File system location of the new ORACLE_HOME (migration destination).
Oracle Home	no default	required	File system location of the current ORACLE_HOME.
Oracle OS User	oracle	required	The OS user that owns the specified Oracle Home.
Oracle Version	no default	optional	Version of the Oracle Installation

The Advanced Database Patching Solution

The Database and Middleware Automation (DMA) Database Compliance solution provides tools that you can use to patch specialized Oracle Grid Infrastructure in an efficient and automated way.

The benefits of using this DMA solution instead of patching your databases manually are:

- You can patch databases across multiple targets in either a development or production environment.
- You can use a variety of Oracle-supplied patches.
- You can easily roll back your system to a previous patch level.
- You can reduce database down time.
- You can reduce patching errors thanks to safeguards that DMA provides.

By consistently using the tools provided in this solution, you can apply database patches more accurately and consistently—and save time in the process.

Oracle - Patch Grid Infrastructure and Databases v6

This workflow enables you to patch Oracle Grid Infrastructure on 11.2 and 12.1 environments. The workflow will work for both Grid Standalone and Grid Cluster environments. The workflow is designed to run against the ASM Instance (+ASM, +ASM1) selected as the target and will handle patching any database homes and databases automatically through self discovery.

In order to run on a clustered environment, you must specify a list of all nodes that are part of the Oracle Cluster in the Grid Nodes parameter. If there are specific Oracle Database Homes that you want included or excluded from the patching process, you can expose the Oracle Database Homes parameter in the Gather Advanced Parameters for Patch Grid Infrastructure and Databases step and specify the homes.

To use this workflow in your environment, see the following information:

Topic	Information Included
"Prerequisites for this Workflow"	List of prerequisites that must be satisfied before you can run this workflow
"How this Workflow Works"	Information about what the workflow does, including validation checks performed, and steps executed
"How to Run this Workflow"	Instructions for running this workflow in your environment
"Sample Scenarios"	Examples of typical parameter values for this workflow
"Parameters for Oracle - Patch Grid Infrastructure and Databases v6" on page 357	List of input parameters for this workflow

Note: The documentation for this workflow refers to the workflow and its steps by their base names. The names in the DMA user interface may have a version appended, for example, v2.

Prerequisites for this Workflow

Be sure that the following prerequisites are satisfied before you run the ["Oracle - Patch Grid Infrastructure and Databases v6"](#) workflow:

1. You have installed the DMA Advanced Database Patching solution pack.
2. You have read access to all specified inventory pointers (Linux/UNIX).
3. You have a valid Oracle support contract.
4. You have imported the pertinent Oracle CPU/SPU into the DMA software repository.
5. If you do not specify the OPatch option, you must have the current OPatch already available on your system.
6. Your targets are running one of the supported operating systems (see the *DMA Support Matrix*).

Other Dependencies

- Oracle Grid Home must be version 11.2.0.1 or later.
- The Oracle OPatch utility must be the latest version, or you must provide the newest OPatch archive using the appropriate workflow parameter.
- You must have enough free space available, which varies depending on the Oracle patch.

For more information about prerequisites for Oracle Database, refer to the [Oracle Database Product Documentation](#).

How this Workflow Works

The "Oracle - Patch Grid Infrastructure and Databases v6" workflow performs the following actions:

- The initial steps of the workflow prepare it to patch the Grid Home and all of the Database Homes and databases managed with Grid. The workflow performs the validation checks described in the "Validation Checks Performed" section below.
- If an OPatch archive file has been provided, the workflow uses the correct OPatch version to patch the Oracle OPatch utility before applying the patch to the Grid Infrastructure Home and the target databases.
- The workflow performs various staging operations before applying the patch such as checking to see if Oracle Home is to be patched. If so, it will perform various validation checks. Otherwise, it will perform just those staging operations relevant to patching the Grid Infrastructure Home.
- The workflow applies the patch to the Grid Home and to all of the Database Homes and databases managed with the Grid.
- The final steps of the workflow allow the workflow to end cleanly. The workflow verifies that the patch has been applied. Then it cleans up the downloaded files and runs Discovery to update the metadata.

Validation Checks Performed

This workflow validate the following conditions:

1. The input parameters have the proper syntax (no special characters or spaces).
2. Files exist or have valid specifications.
3. The current Oracle Database and OPatch versions match the required versions.
4. The supplied patch applies to Oracle Home.
5. Recompiled database views are accurate.
6. The download location has enough space.

After the patching operation is completed, the workflow verifies that the patch has been successfully applied to the Grid Infrastructure Home, Database Homes, and the target databases.

Steps Executed

The "Oracle - Patch Grid Infrastructure and Databases v6" workflow includes the following steps. Each step must complete successfully before the next step can start. If a step fails, the workflow reports a failure and all subsequent steps are skipped.

Steps Used in Oracle - Patch Grid Infrastructure and Databases

Workflow Step	Description
Gather Parameters for Patch Grid Infrastructure and Databases v2	This step gathers the required parameters for Oracle - Patch Grid Infrastructure and Databases.
Gather Advanced Parameters for Patch Grid Infrastructure and Databases v5	This step gathers the optional advanced parameters for Oracle - Patch Grid Infrastructure and Databases.
Prepare Oracle Instance	This step prepares instance level Oracle access.
Validate Patch Grid Infrastructure and Databases v6	This step validates the values specified for the input parameters used by Oracle - Patch Grid Infrastructure and Databases. It also sets the values of various output parameters that will be consumed by subsequent steps.
Download Software	This step downloads a list of files to a specified location on the target server.
Unzip for Patch Grid Infrastructure and Databases v5	This step unzips on all nodes: <ul style="list-style-type: none"> • The OPatch on the Grid and the Database Homes • The Patch Archive
Patch Grid Infrastructure and Databases v5	This step runs the preparatory SQL script and then patches the Grid infrastructure, the Database Homes, and all databases managed with the Grid.
Cleanup Downloaded Files v2	This step removes files and archives that were downloaded to the target system during previous workflow steps.
Determine Oracle Patch Info	This step determines all patch information that the workflow requires to apply the pertinent patch.
Verify Grid and Databases Patched v4	This step confirms that the patch has been properly applied to the Grid Infrastructure, Database Homes, and databases managed with the Grid. In a clustered environment, the workflow verifies across all nodes.
Run slibclean	This step runs the <code>slibclean</code> command on AIX targets. The <code>slibclean</code> utility removes any currently unused modules in kernel and library memory.
Cleanup Downloaded Files v2	This step removes all downloaded files and archives.
Backup and Compress v2	By default this step backs up all of the Grid and Database Homes and then compresses them into an archive. In addition, you can specify other directories and files that you want backed up—these parameters can be found in Gather Advanced Parameters for Patch Grid Infrastructure and Databases
Discover Oracle Databases	This step audits the server's physical environment looking for Oracle instances and databases. <p>Note: Discovery is only additive. It will not remove instances or</p>

Steps Used in Oracle - Patch Grid Infrastructure and Databases, continued

Workflow Step	Description
	<p>databases currently in your environment. It is the end user's responsibility to delete content this is no longer in use.</p> <p>In cluster situations where on node is active and other nodes are inactive, Discovery will only find instances and databases on the active node. Nothing will be added to inactive nodes.</p>

Note: For input parameter descriptions and defaults, see ["Parameters for Oracle - Patch Grid Infrastructure and Databases v6"](#) on page 357.

How to Run this Workflow

The following instructions show you how to customize and run the ["Oracle - Patch Grid Infrastructure and Databases v6"](#) workflow in your environment.

The workflow provides default values for some parameters. These default values are usually sufficient for a "typical" installation. You can override the defaults by specifying parameter values in the deployment. You can also expose additional parameters in the workflow, if necessary, to accomplish more advanced scenarios. Any parameters not explicitly specified in the deployment will have the default values listed in ["Parameters for Oracle - Patch Grid Infrastructure and Databases v6" on page 357](#).

Note: Before following this procedure, review the ["Prerequisites for this Workflow" on page 342](#), and ensure that all requirements are satisfied.

To use the Oracle - Patch Grid Infrastructure and Databases workflow:

1. Create a deployable copy of the workflow.
2. Determine the values that you will specify for the following parameters:

Input Parameters Defined in this Step: Gather Parameters for Patch Grid Infrastructure and Databases v2

Parameter Name	Default Value	Required	Description
Gold Grid Home	no default	required	A .tgz home that is already patched to be unzipped and then migrated to. This parameter is to be used in place of using a patch archive.
Gold RDBMS Home	no default	required	A .tgz home that is already patched to be unzipped and then migrated to either now or at a later date. This parameter is to be used instead of Patch Archive parameter. Multiple homes can be provided separating each home:version combination with a comma. For example: home1.tgz:12102,home2.tgz:11204
Oracle OS User	no default	required	Oracle OS user.
Patch Archive	no default	required	Comma-separated list of patch file names (not fully-qualified).

Additional Input Parameters Defined in this Step: Gather Advanced Parameters for Patch Grid Infrastructure and Databases v5

Parameter Name	Default Value	Required	Description
2 Phase Patching	false	optional	If the value is True the workflow will clone and patch the cloned home in the first run of the workflow. The second time you run the workflow it will perform the switchover operation to the newly patched home.
Additional Grid Patches	no default	optional	Comma separated list of any additional patched that need to be applied on top of the PSU. Example are ocw patches or any oneoff patches that need to be applied to the Grid Home.
Backup File List	see description	optional	List of additional files and folders that you would like backed up. By default, the backup already includes Grid Home, Database Homes, and Inventory Location.
Backup File Name	dma_backup	optional	Name of the backup file.
Backup Location	no default	optional	Location where the backup file will be located.
Cleanup	True	optional	If true, the workflow will cleanup downloaded and extracted files upon completion. Valid values are True and False.
Clone Patching Database	no default	optional	True if patching process should use Oracle Clone Patching process for Oracle Database Homes and Databases.
Clone Patching Grid	no default	optional	True if patching process should use Oracle Clone Patching process for Oracle Database Homes and Databases.
DB Version	no default	optional	The current Oracle Database version. For example: 11.2.0.3
Decommission Grid Home	true	optional	If Clone Patching Grid is set to True this parameter if set to true will decommission old Grid Home. If set to False the old Grid Home will remain after workflow has completed.
Decommission RDBMS Home	true	optional	If Clone Patching Database is set to True this parameter if set to True will decommission any old RDBMS Homes. If set to False the old RDBMS Homes will remain after workflow has completed.
Download Location	/tmp	optional	Location where all files where files will be downloaded or they already exist.
Extract Location	/tmp	optional	Directory location where the ZIP archives will be extracted.

Additional Input Parameters Defined in this Step: Gather Advanced Parameters for Patch Grid Infrastructure and Databases v5, continued

Parameter Name	Default Value	Required	Description
Grid Nodes	no default	optional	Comma separated list of nodes that are part of a Grid Infrastructure environment. By default, the nodes are discovered by <code>olsnodes</code> and then all nodes are rolled back.
Ignorable Oracle Errors	no default	optional	A comma-separated list of Oracle errors to be ignored when applying the patch to the database. This is in addition to the list of Oracle errors specified in the patch readme file. Values are of the form <code>ORA-nnnnn</code> . For example: <code>ORA-04020,ORA-03113</code>
Migrate Database	true	optional	When using a Gold RDBMS Home to patch, the databases for the homes will be migrated to the new home and patched. Default value is True. To migrate and patched databases rather than during the workflow specify False and run the Oracle - Migrate and Patch Grid Managed Database.
OCM Response File	no default	optional	Path name of the Oracle Configuration Manager (OCM) response file. If not found on the target, this file is downloaded from the software repository. If left blank, a default response file will be created.
OPatch Archive	no default	optional	The OPatch Archive file required for this patch (not fully-qualified). If this parameter value is not specified, the current OPatch version will be used.
OPatch Version	no default	optional	The new OPatch version of the patch being applied. If you specify a value for this parameter, you MUST also specify values for Patch Number and Patch Name.
Oneoff Archives	no default	optional	Comma separated list of One-off patch archive (s).
Oracle Database Homes	ALL	optional	Oracle Database Homes to patch along with the Oracle Grid. Valid values are ALL, NONE, INCLUDE: followed by a comma separated list of Oracle Homes to patch with the Oracle Grid, and EXCLUDE: followed by a comma separated list of Oracle Homes to exclude from the patching process.
Oracle Group	no default	optional	The group that owns the Grid Oracle Home.
Override Current OPatch Version	False	optional	If the value is True, the existing OPatch version will be overridden by the supplied OPatch archive version.

Additional Input Parameters Defined in this Step: Gather Advanced Parameters for Patch Grid Infrastructure and Databases v5, continued

Parameter Name	Default Value	Required	Description
Patch Information File	no default	optional	Supplementary patch information supplied by support. If this file is not found on the target, it is downloaded from the software repository on the DMA server.
Patch Name	no default	optional	Name of the patch that is being applied.
Patch Number	no default	optional	Patch number of the patch being applied.
Preparatory SQL	no default	optional	File name that contains SQL statements that must be run before the database catalog update. This file is passed directly to SQLPlus and must be formatted as such. If not found on the target, it is downloaded from the software repository.
RDBMS Homes Only	false	optional	If value is True than the patching workflow will only patch database homes found to be patched from the Oracle Database Homes parameter. The default value is False.
Required Disk Space	no default	optional	Amount of disk space required (checked for) before installing the patch. Size is in Gigabytes.
Run Database View Recompile	N	optional	If set to Y, the Database View Recompile step will be run. Valid values are Y and N.
Startup Instance	Y	optional	If set to Y, the workflow will attempt to start the database instance if it is offline. Valid values are Y and N.
Trust SSL Certificates	no default	optional	If this parameter is set to True, the workflow will trust any Secure Sockets Layer (SSL) certificate used to connect to the HP DMA web service.
Web Service Password	no default	optional	Password for the DMA Discovery web service API.
Web Service URL	no default	optional	URL for the DMA Discovery web service API.
Web Service User	no default	optional	User who is capable of modifying the managed environment by using the DMA Discovery web service API.

Note: This is the minimum set of parameters required to run this workflow. You may specify values for the optional advanced parameters and you may need to expose additional parameters depending on your objectives.

See ["Parameters for Oracle - Patch Grid Infrastructure and Databases v6" on page 357](#) for detailed descriptions of all input parameters for this workflow, including default values.

3. In the workflow editor, expose any additional parameters that you need. You will specify values for those parameters when you create the deployment.
4. Save the changes to the workflow (click **Save** in the lower right corner).
5. Create a new deployment.
6. On the Parameters tab, specify values for the required parameters listed in step 2 and any additional parameters that you have exposed. You do not need to specify values for those parameters whose default values are appropriate for your environment.
7. On the Targets tab, specify one or more targets for this deployment.
8. Save the deployment (click **Save** in the lower right corner).
9. Run the workflow using this deployment.

To verify the results:

The workflow will complete and report SUCCESS on the Console if it has run successfully. If an error occurs during workflow execution, the error is logged, and the workflow terminates in the FAILURE state.

Optional: To further verify that the Grid patch was successfully applied:

1. Log in to the target server.
2. Set the ORACLE_HOME to your Grid Home.
3. Run the command: `$ORACLE_HOME/OPatch/patch lsinventory`
4. Verify that the patch number from the archive that you specified is listed in the output.

Optional: To further verify that the patch was successfully applied on the Database Homes:

1. Log in to the target server.
2. Set the ORACLE_HOME to your Database Home.
3. Run the command: `$ORACLE_HOME/OPatch/patch lsinventory`
4. Verify that the patch number from the archive that you specified is listed in the output.

Optional: To further verify that the patch was successfully applied to the Oracle Database Instances associated with the Oracle Home:

1. Log in as an SQLPlus privileged user.
2. Set the environment variable, for example:


```
. oraenv
```
3. Give the name of the Oracle Database, for example:


```
orca
```
4. Search results for comments and actions, for example:


```
select comments,action from sys.registry$history;
```
5. Check that the desired patch was applied. For example, look for:


```
CPUOct2013 or PSUOct2013
```

Sample Scenarios

This topic shows you how to use various parameters to achieve the following advanced patching scenarios in your environment using the "Oracle - Patch Grid Infrastructure and Databases v6" workflow.

Scenario 1: In-Place Patching

This option patches GI, any database homes, and databases that have been included based on parameter inputs for the "Oracle Database Homes" parameter. The parameters used for In-Place patching are as follows:

Parameter Name	Value
2 Phase Patching	False
Clone Patching Database	False
Clone Patching Grid	False
Oracle Database Homes	ALL
RDBMS Homes Only	False

Scenario 2: Clone Patching Single Phase

This option clones grid and database home(s) that are specified to be patched. Once cloned, the patches will be applied to the cloned home. After patching is complete for grid and database homes, switchover occurs to move grid services and database services to the newly patched homes. The parameters used for Clone Patching Single Phase are as follows:

Parameter Name	Value
2 Phase Patching	False
Clone Patching Database	True
Clone Patching Grid	True
Oracle Database Homes	ALL
RDBMS Homes Only	False

Scenario 3: Clone Patching Two Phase

This option clones grid and database home(s) that are specified to be patched. Once cloned, the patches will be applied to the cloned home. The workflow will then exit. The second phase is to re-run the workflow at which point the workflow will identify the first phase of the workflow has been executed and executes the switchover operations to move services to the new patched homes. The parameters used for Clone Patching Two Phase are as follows:

Parameter Name	Value
2 Phase Patching	True
Clone Patching Database	True
Clone Patching Grid	True
Oracle Database Homes	ALL
RDBMS Homes Only	False

Scenario 4: Patch RDBMS Home(s) Only

This option can be used to patch database homes of a different version at a later date separate from patching grid. This parameter can still be used with clone patching but will only effect the specified database home(s) part of the deployment. The parameters used for Clone Patching Two Phase are as follows:

Parameter Name	Value
2 Phase Patching	False
Clone Patching Database	True
Clone Patching Grid	True
Oracle Database Homes	ALL
RDBMS Homes Only	False

The following options are available for Oracle Database Homes parameter:

- ALL – This option patches every Oracle Database Home found on the selected target.
- NONE – This option only patches grid and leaves all database homes as is.
- INCLUDE:/u01/app/oracle/product/11.2.0/home_1,/u01/app/oracle/product/11.2.0/home_2 – This option lets you specify only specific home(s) that should be patched with grid.
- EXCLUDE:/u01/app/oracle/product/11.2.0/home_1,/u01/app/oracle/product/11.2.0/home_2 – This Option lets you specify only specific home(s) that should be excluded while patching grid.

Scenario 5: One Off Patching

One off patches can be applied using this workflow by specifying the one or many one off patches to be applied after the PSU. The parameter takes a comma separated list of one off patch archive provided by Oracle.

Parameter Name	Value
Oneoff Archives	p16836674_112040_Linux-x86-64.zip,p13571876_112046_Linux-x86-64.zip,p14059190_112040_Generic.zip

If any of the one-off patches require post scripts to be run, you have to create a function library called “oraclepatchoneoff”. Contents of the function should be formatted as follows:

```
one_off_patch_info = {

'13571876': {'Patch Name': '13571876', 'Database Version': '11.2.0.4.6', 'Oracle
Errors': ['ORA-29809', 'ORA-29931', 'ORA-29830', 'ORA-00942', 'ORA-00955', 'ORA-
01430', 'ORA-01432', 'ORA-01434', 'ORA-01435', 'ORA-01917', 'ORA-01920', 'ORA-
01921', 'ORA-01952', 'ORA-02303', 'ORA-02443', 'ORA-04043', 'ORA-29832', 'ORA-
29844', 'ORA-14452', 'ORA-06512', 'ORA-01927'], 'OPatch Version': '11.2.0.3.5',
'Additional Patches': '', 'SQL Script': ''},

'14059190': {'Patch Name': '14059190', 'Database Version': '11.2.0.4.0', 'Oracle
Errors': ['ORA-29809', 'ORA-29931', 'ORA-29830', 'ORA-00942', 'ORA-00955', 'ORA-
01430', 'ORA-01432', 'ORA-01434', 'ORA-01435', 'ORA-01917', 'ORA-01920', 'ORA-
01921', 'ORA-01952', 'ORA-02303', 'ORA-02443', 'ORA-04043', 'ORA-29832', 'ORA-
29844', 'ORA-14452', 'ORA-06512', 'ORA-01927'], 'OPatch Version': '11.2.0.3.5',
'Additional Patches': '', 'SQL Script': '<Patch Dir>/14059190/postinstall.sql'},

'16836674': {'Patch Name': '16836674', 'Database Version': '11.2.0.4.0', 'Oracle
Errors': ['ORA-29809', 'ORA-29931', 'ORA-29830', 'ORA-00942', 'ORA-00955', 'ORA-
01430', 'ORA-01432', 'ORA-01434', 'ORA-01435', 'ORA-01917', 'ORA-01920', 'ORA-
01921', 'ORA-01952', 'ORA-02303', 'ORA-02443', 'ORA-04043', 'ORA-29832', 'ORA-
29844', 'ORA-14452', 'ORA-06512', 'ORA-01927'], 'OPatch Version': '11.2.0.3.5',
'Additional Patches': '', 'SQL Script': ''},

}
```

Scenario 6: OJVM Patching

OJVM patches can be applied using this workflow by specifying the OJVM archive as input to ‘Oneoff Archives’ parameters. The OJVM patch will be applied after PSU.

Parameter Name	Value
Oneoff Archives	p22674697_112040_Linux-x86-64.zip

For OJVM patches it is mandatory to create a function named “oraclepatchoneoff”. The ‘postinstall.sql’ script needs to be provided as value for ‘SQL Script’ for the given OJVM patch number. Contents of the function should be formatted as follows:

```
one_off_patch_info = {

'22674697': {'Patch Name': '22674697', 'Database Version': '11.2.0.4.0', 'Oracle
Errors': ['ORA-29809', 'ORA-29931', 'ORA-29830', 'ORA-00942', 'ORA-00955', 'ORA-
01430', 'ORA-01432', 'ORA-01434', 'ORA-01435', 'ORA-01917', 'ORA-01920', 'ORA-
```

```

01921', 'ORA-01952', 'ORA-02303', 'ORA-02443', 'ORA-04043', 'ORA-29832', 'ORA-
29844', 'ORA-14452', 'ORA-06512', 'ORA-01927'], 'OPatch Version': '11.2.0.3.5',
'Additional Patches': '', 'SQL Script': '<Patch Dir>/22674697/postinstall.sql'},

'22139245': {'Patch Name': '22139245', 'Database Version': '11.2.0.4.0', 'Oracle
Errors': ['ORA-29809', 'ORA-29931', 'ORA-29830', 'ORA-00942', 'ORA-00955', 'ORA-
01430', 'ORA-01432', 'ORA-01434', 'ORA-01435', 'ORA-01917', 'ORA-01920', 'ORA-
01921', 'ORA-01952', 'ORA-02303', 'ORA-02443', 'ORA-04043', 'ORA-29832', 'ORA-
29844', 'ORA-14452', 'ORA-06512', 'ORA-01927'], 'OPatch Version': '11.2.0.3.5',
'Additional Patches': '', 'SQL Script': '<Patch Dir>/22139245/postinstall.sql'},
}

```

Be sure that the default values for all remaining input parameters are appropriate for your environment (see ["Parameters for Oracle - Patch Grid Infrastructure and Databases v6" on page 357](#)).

Scenario 2: Apply patch to a Grid Standalone environment

In this scenario, the workflow patches a Grid Standalone environment. It applies the patch to both the Grid Standalone Home, the Oracle Database Homes, and all associated databases. You only need to leave Grid Nodes blank.

Parameter Name	Description
Patch Archive	Comma-separated list of patch file names (not fully-qualified). Example: p17272829_121010_Linux-x86-64.zip
Grid Nodes	Comma separated list of nodes that are part of a Grid Infrastructure environment. By default, the nodes are discovered by olsnodes and then all nodes are rolled back. Example:
OPatch Archive	The OPatch Archive file required for this patch (not fully-qualified). If this parameter value is not specified, the current OPatch version will be used. Example: p6880880_121010_Linux-x86-64.zip
Oracle Database Homes	Oracle Database Homes to patch along with the Oracle Grid. Valid values are ALL, NONE, INCLUDE: followed by a comma separated list of Oracle Homes to patch with the Oracle Grid, and EXCLUDE: followed by a comma separated list of Oracle Homes to exclude from the patching process. Example: ALL
Patch Information File	Supplementary patch information supplied by support. If this file is not found on the target, it is downloaded from the software repository on the DMA server. Example: 201310_PatchInfo.xml

Be sure that the default values for all remaining input parameters are appropriate for your environment (see ["Parameters for Oracle - Patch Grid Infrastructure and Databases v6" on page 357](#)).

Scenario 3: Only patch specific Oracle Database Homes

In this scenario, the workflow patches Grid clustered environments. It applies the patch to the Grid Infrastructure, only the specified Oracle Database Homes, and all associated databases. You only need to set Oracle Database Homes to the desired Oracle Database Homes.

Parameter Name	Description
Patch Archive	Comma-separated list of patch file names (not fully-qualified). Example: p17272829_121010_Linux-x86-64.zip
Grid Nodes	Comma separated list of nodes that are part of a Grid Infrastructure environment. By default, the nodes are discovered by olsnodes and then all nodes are rolled back. Example: dma-rac1.usa.hp.com,dma-rac2.usa.hp.com
OPatch Archive	The OPatch Archive file required for this patch (not fully-qualified). If this parameter value is not specified, the current OPatch version will be used. Example: p6880880_121010_Linux-x86-64.zip
Oracle Database Homes	Oracle Database Homes to patch along with the Oracle Grid. Valid values are ALL, NONE, INCLUDE: followed by a comma separated list of Oracle Homes to patch with the Oracle Grid, and EXCLUDE: followed by a comma separated list of Oracle Homes to exclude from the patching process. Example: INCLUDE: /u01/app/oracle/product/12.1.0/dbhome_1
Patch Information File	Supplementary patch information supplied by support. If this file is not found on the target, it is downloaded from the software repository on the DMA server. Example: 201310_PatchInfo.xml

Be sure that the default values for all remaining input parameters are appropriate for your environment (see ["Parameters for Oracle - Patch Grid Infrastructure and Databases v6" on the next page](#)).

Parameters for Oracle - Patch Grid Infrastructure and Databases v6

The following tables describe the required and optional input parameters for this workflow. Some of these parameters are not initially visible in a deployment. For most parameters, if you do not specify a value for a parameter, a default value is assigned.

Input Parameters Defined in this Step: Gather Parameters for Patch Grid Infrastructure and Databases v2

Parameter Name	Default Value	Required	Description
Gold Grid Home	no default	required	A .tgz home that is already patched to be unzipped and then migrated to. This parameter is to be used in place of using a patch archive.
Gold RDBMS Home	no default	required	A .tgz home that is already patched to be unzipped and then migrated to either now or at a later date. This parameter is to be used instead of Patch Archive parameter. Multiple homes can be provided separating each home:version combination with a comma. For example: home1.tgz: 12102,home2.tgz: 11204
Oracle OS User	no default	required	Oracle OS user.
Patch Archive	no default	required	Comma-separated list of patch file names (not fully-qualified).

Additional Input Parameters Defined in this Step: Gather Advanced Parameters for Patch Grid Infrastructure and Databases v5

Parameter Name	Default Value	Required	Description
2 Phase Patching	false	optional	If the value is True the workflow will clone and patch the cloned home in the first run of the workflow. The second time you run the workflow it will perform the switchover operation to the newly patched home.
Additional Grid Patches	no default	optional	Comma separated list of any additional patched that need to be applied on top of the PSU. Example are ocw patches or any oneoff patches that need to be applied to the Grid Home.
Backup File List	see description	optional	List of additional files and folders that you would like backed up. By default, the backup already includes Grid Home, Database Homes, and Inventory Location.
Backup File Name	dma_backup	optional	Name of the backup file.
Backup Location	no default	optional	Location where the backup file will be located.
Cleanup	True	optional	If true, the workflow will cleanup downloaded and extracted files upon completion. Valid values are True and False.

Additional Input Parameters Defined in this Step: Gather Advanced Parameters for Patch Grid Infrastructure and Databases v5, continued

Parameter Name	Default Value	Required	Description
Clone Patching Database	no default	optional	True if patching process should use Oracle Clone Patching process for Oracle Database Homes and Databases.
Clone Patching Grid	no default	optional	True if patching process should use Oracle Clone Patching process for Oracle Database Homes and Databases.
DB Version	no default	optional	The current Oracle Database version. For example: 11.2.0.3
Decommission Grid Home	true	optional	If Clone Patching Grid is set to True this parameter if set to true will decommission old Grid Home. If set to False the old Grid Home will remain after workflow has completed.
Decommission RDBMS Home	true	optional	If Clone Patching Database is set to True this parameter if set to True will decommission any old RDBMS Homes. If set to False the old RDBMS Homes will remain after workflow has completed.
Download Location	/tmp	optional	Location where all files where files will be downloaded or they already exist.
Extract Location	/tmp	optional	Directory location where the ZIP archives will be extracted.
Grid Nodes	no default	optional	Comma separated list of nodes that are part of a Grid Infrastructure environment. By default, the nodes are discovered by <code>olsnodes</code> and then all nodes are rolled back.
Ignorable Oracle Errors	no default	optional	A comma-separated list of Oracle errors to be ignored when applying the patch to the database. This is in addition to the list of Oracle errors specified in the patch readme file. Values are of the form ORA-nnnnn. For example: ORA-04020,ORA-03113
Migrate Database	true	optional	When using a Gold RDBMS Home to patch, the databases for the homes will be migrated to the new home and patched. Default value is True. To migrate and patched databases rather than during the workflow specify False and run the Oracle - Migrate and Patch Grid Managed Database.
OCM Response File	no default	optional	Path name of the Oracle Configuration Manager (OCM) response file. If not found on the target, this file is downloaded from the software repository. If left blank, a default response file will be created.
OPatch Archive	no default	optional	The OPatch Archive file required for this patch (not fully-qualified). If this parameter value is not specified, the current OPatch version will be used.
OPatch Version	no default	optional	The new OPatch version of the patch being applied. If you specify a value for this parameter, you MUST also

Additional Input Parameters Defined in this Step: Gather Advanced Parameters for Patch Grid Infrastructure and Databases v5, continued

Parameter Name	Default Value	Required	Description
			specify values for Patch Number and Patch Name.
Oneoff Archives	no default	optional	Comma separated list of One-off patch archive(s).
Oracle Database Homes	ALL	optional	Oracle Database Homes to patch along with the Oracle Grid. Valid values are ALL, NONE, INCLUDE: followed by a comma separated list of Oracle Homes to patch with the Oracle Grid, and EXCLUDE: followed by a comma separated list of Oracle Homes to exclude from the patching process.
Oracle Group	no default	optional	The group that owns the Grid Oracle Home.
Override Current OPatch Version	False	optional	If the value is True, the existing OPatch version will be overridden by the supplied OPatch archive version.
Patch Information File	no default	optional	Supplementary patch information supplied by support. If this file is not found on the target, it is downloaded from the software repository on the DMA server.
Patch Name	no default	optional	Name of the patch that is being applied.
Patch Number	no default	optional	Patch number of the patch being applied.
Preparatory SQL	no default	optional	File name that contains SQL statements that must be run before the database catalog update. This file is passed directly to SQLPlus and must be formatted as such. If not found on the target, it is downloaded from the software repository.
RDBMS Homes Only	false	optional	If value is True then the patching workflow will only patch database homes found to be patched from the Oracle Database Homes parameter. The default value is False.
Required Disk Space	no default	optional	Amount of disk space required (checked for) before installing the patch. Size is in Gigabytes.
Run Database View Recompile	N	optional	If set to Y, the Database View Recompile step will be run. Valid values are Y and N.
Startup Instance	Y	optional	If set to Y, the workflow will attempt to start the database instance if it is offline. Valid values are Y and N.
Trust SSL Certificates	no default	optional	If this parameter is set to True, the workflow will trust any Secure Sockets Layer (SSL) certificate used to connect to the HP DMA web service.
Web Service Password	no default	optional	Password for the DMA Discovery web service API.
Web Service URL	no default	optional	URL for the DMA Discovery web service API.
Web Service User	no default	optional	User who is capable of modifying the managed

Additional Input Parameters Defined in this Step: Gather Advanced Parameters for Patch Grid Infrastructure and Databases v5, continued

Parameter Name	Default Value	Required	Description
			environment by using the DMA Discovery web service API.

Oracle - Rollback Patch from Grid Infrastructure and Database

This workflow rolls back a patch from Oracle Grid Infrastructure on 11.2 and 12.1 environments. It works for both Grid Standalone and Grid Cluster environments. In addition to the Grid Home, it rolls back the patch from all of the Database Homes and databases managed with the Grid.

In order to run on a clustered environment, in the Grid Nodes parameter you specify a list all nodes that are part of the Oracle Cluster.

To use this workflow in your environment, see the following information:

Topic	Information Included
"Prerequisites for this Workflow"	List of prerequisites that must be satisfied before you can run this workflow
"How this Workflow Works"	Information about what the workflow does, including validation checks performed, and steps executed
"How to Run this Workflow"	Instructions for running this workflow in your environment
"Sample Scenarios"	Examples of typical parameter values for this workflow
"Parameters for Oracle - Rollback Patch from Grid Infrastructure and Database" on page 370	List of input parameters for this workflow

Note: The documentation for this workflow refers to the workflow and its steps by their base names. The names in the DMA user interface may have a version appended, for example, v2.

Prerequisites for this Workflow

Be sure that the following prerequisites are satisfied before you run the ["Oracle - Rollback Patch from Grid Infrastructure and Database"](#) workflow:

1. You have installed the DMA Advanced Database Patching solution pack.
2. You have Read access to all specified inventory pointers (Linux/UNIX).
3. Your targets are running one of the supported operating systems (see the *DMA Support Matrix*).

Other Dependencies

- The workflow must have unchallenged ability to become the Oracle database user (typically oracle) on all nodes of the RAC. This is generally done using `sudo` or `ssh oracle@localhost`.
- The workflow must have unchallenged ability to become the Oracle CRS user (example oracrs) on all nodes of the RAC. This is generally done using `sudo` or `ssh oracle@localhost`.
- The workflow must have unchallenged ability to become the superuser user (typically root) on all nodes of the RAC. This is generally done using `sudo` or `ssh oracle@localhost`.
- The workflow and the CRS/ASM/Instance/Listener users (typically oracle) must have unchallenged ability to `ssh` to all the RAC nodes.

For more information about prerequisites for Oracle Database, refer to the [Oracle Database Product Documentation](#).

How this Workflow Works

The "Oracle - Rollback Patch from Grid Infrastructure and Database" workflow performs the following actions:

- The initial steps of the workflow prepare it to roll back the patch from the Grid Home, and all of the Database Homes and databases managed with Grid. The workflow performs the validation checks described in the "Validation Checks Performed" section below.
- The workflow verifies the archive to roll back, the download location, and the Homes to roll back.
- The workflow rolls back the patch from the Grid Home and from all of the Database Homes and databases managed with the Grid.
- The final steps of the workflow allow the workflow to end cleanly. The workflow verifies that the patch has been rolled back. Then it runs Discovery to update the metadata and cleans up the downloaded files.

Validation Checks Performed

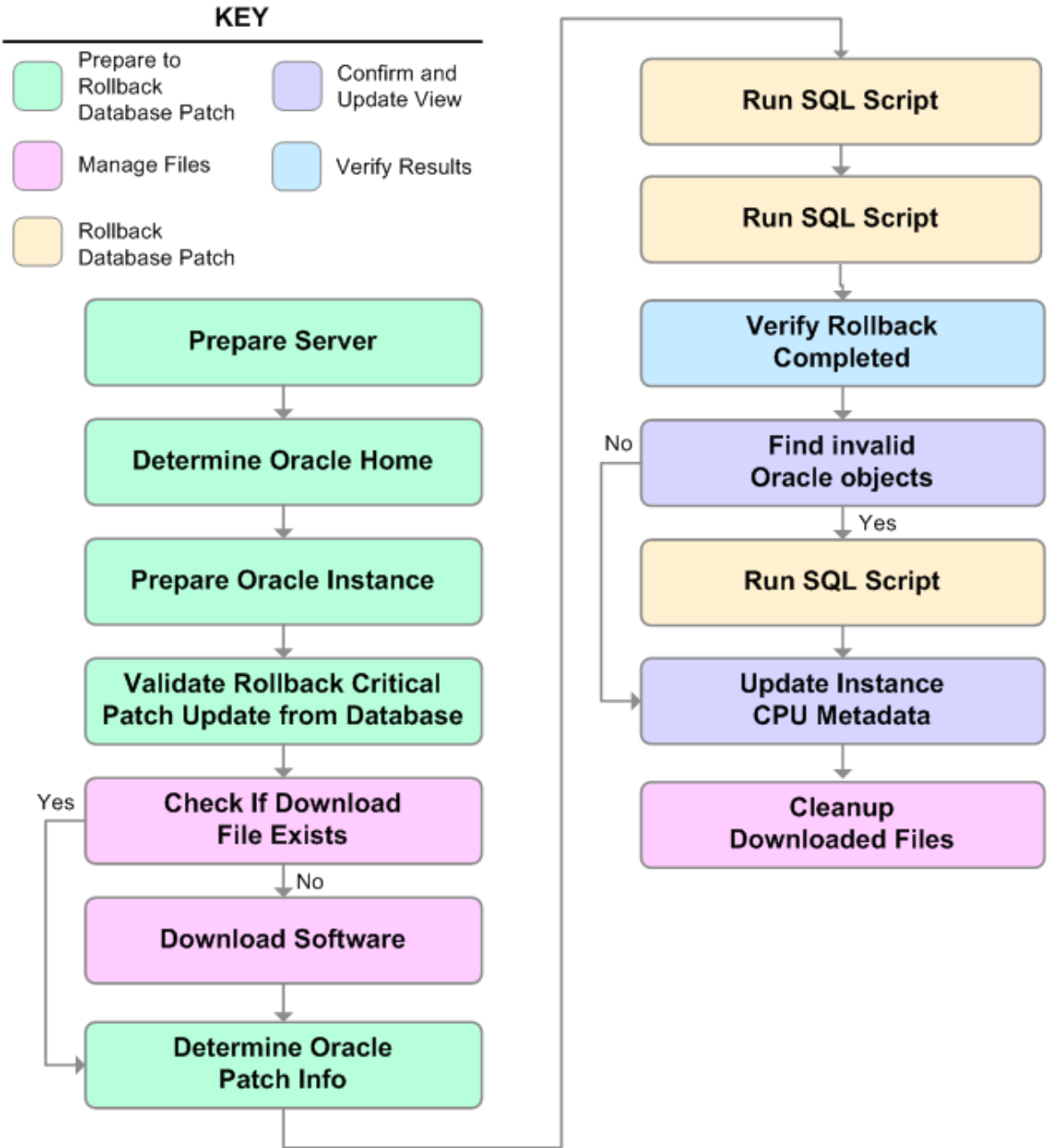
This workflow validates the following conditions:

1. The input parameters have the proper syntax (no special characters or spaces).
2. Files exist or have valid specifications.
3. The supplied patch applies to Oracle Home.
4. The download location has enough space.

After the patching operation is completed, the workflow verifies that the patch has been successfully rolled back from the Grid Infrastructure Home, Database Homes, and the target databases.

Steps Executed

The "Oracle - Rollback Patch from Grid Infrastructure and Database" workflow includes the following steps. Each step must complete successfully before the next step can start. If a step fails, the workflow reports a failure and all subsequent steps are skipped.



Steps Used in Oracle - Rollback Patch from Grid Infrastructure and Databases

Workflow Step	Description
Gather Parameters for Rollback Patch from Grid	This step gathers the required parameters for Oracle - Rollback Patch from Grid Infrastructure and Databases.

Steps Used in Oracle - Rollback Patch from Grid Infrastructure and Databases, continued

Workflow Step	Description
Infrastructure and Databases	
Gather Advanced Parameters for Rollback Patch from Grid Infrastructure and Databases	This step gathers the optional advanced parameters for Oracle - Rollback Patch from Grid Infrastructure and Databases.
Prepare Oracle Instance	This step prepares instance level Oracle access.
Validate Rollback Patch from Grid Infrastructure and Databases	This step validates the parameters for Oracle - Rollback Patch from Grid Infrastructure and Databases.
Download Software	This step downloads a list of files to a specified location on the target server.
Run slibclean	This step runs the <code>slibclean</code> command on AIX targets. The <code>slibclean</code> utility removes any currently unused modules in kernel and library memory.
Rollback Patch Grid Infrastructure and Databases	This step rolls back the patches from the Grid infrastructure, the Database Homes, and all databases managed with the Grid.
Verify Grid and Databases Patch Rollback	This step confirms that the patch has been properly rolled back from the Grid Infrastructure, Database Homes, and databases managed with the Grid. In a clustered environment, the workflow verifies across all nodes.
Discover Oracle Databases	<p>This step audits the server's physical environment looking for Oracle instances and databases.</p> <p>Note: Discovery is only additive. It will not remove instances or databases currently in your environment. It is the end user's responsibility to delete content this is no longer in use.</p> <p>In cluster situations where one node is active and other nodes are inactive, Discovery will only find instances and databases on the active node. Nothing will be added to inactive nodes.</p>
Cleanup Downloaded Files	This step removes files and archives that were downloaded to the target system during previous workflow steps.

Note: For input parameter descriptions and defaults, see ["Parameters for Oracle - Rollback Patch from Grid Infrastructure and Database" on page 370](#).

How to Run this Workflow

The following instructions show you how to customize and run the ["Oracle - Rollback Patch from Grid Infrastructure and Database"](#) workflow in your environment.

Tip: For detailed instructions to run DMA workflows—using the Oracle - Compliance Audit workflow as an example—see DMA Quick Start Tutorial.

The workflow provides default values for some parameters. These default values are usually sufficient for a "typical" installation. You can override the defaults by specifying parameter values in the deployment. You can also expose additional parameters in the workflow, if necessary, to accomplish more advanced scenarios. Any parameters not explicitly specified in the deployment will have the default values listed in ["Parameters for Oracle - Rollback Patch from Grid Infrastructure and Database" on page 370](#).

Note: Before following this procedure, review the ["Prerequisites for this Workflow" on page 362](#), and ensure that all requirements are satisfied.

To use the Oracle - Rollback Patch from Grid Infrastructure and Databases workflow:

1. Create a deployable copy of the workflow.
2. Determine the values that you will specify for the following parameters:

Input Parameters Defined in this Step: Gather Parameters for Rollback Patch from Grid Infrastructure and Databases

Parameter Name	Default Value	Required	Description
Patch Archive	no default	required	Patch archive file of the applied patch to roll back from the Oracle Grid and databases.

Note: This is the minimum set of parameters required to run this workflow. You may specify values for the optional advanced parameters and you may need to expose additional parameters depending on your objectives.

See ["Parameters for Oracle - Rollback Patch from Grid Infrastructure and Database"](#) for detailed descriptions of all input parameters for this workflow, including default values.

3. In the workflow editor, expose any additional parameters that you need. You will specify values for those parameters when you create the deployment.
4. Save the changes to the workflow (click **Save** in the lower right corner).
5. Create a new deployment.
6. On the Parameters tab, specify values for the required parameters listed in step 2 and any

additional parameters that you have exposed. You do not need to specify values for those parameters whose default values are appropriate for your environment.

7. On the Targets tab, specify one or more targets for this deployment.
8. Save the deployment (click **Save** in the lower right corner).
9. Run the workflow using this deployment.

To verify the results:

The workflow will complete and report SUCCESS on the Console if it has run successfully. If an error occurs during workflow execution, the error is logged, and the workflow terminates in the FAILURE state.

Optional: To further verify that the Grid patch was successfully rolled back:

1. Log in to the target server.
2. Set the ORACLE_HOME to your Grid Home.
3. Run the command: `$ORACLE_HOME/OPatch/patch lsinventory`
4. Verify that the patch number that you rolled back is NOT listed in the output.

Optional: To further verify that the patch was successfully rolled back from the Database Homes:

1. Log in to the target server.
2. Set the ORACLE_HOME to your Database Home.
3. Run the command: `$ORACLE_HOME/OPatch/patch lsinventory`
4. Verify that the patch number that you rolled back is NOT listed in the output.

Optional: To further verify that the patch was successfully rolled back from the Oracle Database Instances associated with the Oracle Home:

1. Log in as an SQLPlus privileged user.
2. Set the environment variable, for example:

```
. oraenv
```

3. Give the name of the Oracle Database, for example:

```
orca
```

4. Search results for comments and actions, for example:

```
select comments,action from sys.registry$history;
```

5. Verify that the patch number that you rolled back is NOT listed in the output, for example:

```
CPUOct2013 or PSUOct2013
```


Sample Scenarios

This topic shows you how to use various parameters to achieve the following advanced patching scenarios in your environment using the ["Oracle - Rollback Patch from Grid Infrastructure and Database"](#) workflow.

Note: Use the ASM instance in your environment as the deployment's target.

Scenario: Roll back patch in a Grid cluster or Grid Standalone environment

In this scenario, the workflow rolls back the patch from the Grid Infrastructure (cluster or Standalone), the Database Homes, and all associated databases.

Parameter Name	Description
Patch Archive	Patch archive file of the applied patch to roll back from the Oracle Grid and databases. Example: p17272829_121010_Linux-x86-64.zip

Be sure that the default values for all remaining input parameters are appropriate for your environment (see ["Parameters for Oracle - Rollback Patch from Grid Infrastructure and Database"](#) on the next page).

Parameters for Oracle - Rollback Patch from Grid Infrastructure and Database

The following tables describe the required and optional input parameters for this workflow. Some of these parameters are not initially visible in a deployment. For most parameters, if you do not specify a value for a parameter, a default value is assigned

Note: Only those parameters that are configurable in a standard deployment are listed here. Input parameters that must be mapped to output parameters of previous steps are not listed.

Input Parameters Defined in this Step: Gather Parameters for Rollback Patch from Grid Infrastructure and Databases

Parameter Name	Default Value	Required	Description
Patch Archive	no default	required	Patch archive file of the applied patch to roll back from the Oracle Grid and databases.

Additional Input Parameters Defined in this Step: Gather Advanced Parameters for Rollback Patch from Grid Infrastructure and Databases

Parameter Name	Default Value	Required	Description
Cleanup	True	optional	If true, the workflow will cleanup downloaded and extracted files upon completion. Valid values are True and False.
Download Location	/tmp	optional	Location where all files where files will be downloaded or they already exist.
Extract Location	/tmp	optional	Directory location where the ZIP archives will be extracted.
Grid Nodes	no default	optional	Comma separated list of nodes that are part of a Grid Infrastructure environment. By default, the nodes are discovered by <code>olsnodes</code> and then all nodes are rolled back.
Ignorable Oracle Errors	no default	optional	A comma-separated list of Oracle errors to be ignored when applying the patch to the database. This is in addition to the list of Oracle errors specified in the patch readme file. Values are of the form <code>ORA-nnnnn</code> . For example: <code>ORA-04020,ORA-03113</code>
OCM Response File	no default	optional	Path name of the Oracle Configuration Manager (OCM) response file. If not found on the target, this file is downloaded from the software repository. If left blank, a default response file will be created.
Oracle Database Homes	ALL	optional	Oracle Database Homes to roll back along with the Oracle Grid. Valid values are <code>ALL</code> , <code>NONE</code> , <code>INCLUDE</code> : followed by a comma separated list of Oracle Homes to roll back with the Oracle Grid, and <code>EXCLUDE</code> : followed by a comma separated list of Oracle Homes to

Additional Input Parameters Defined in this Step: Gather Advanced Parameters for Rollback Patch from Grid Infrastructure and Databases, continued

Parameter Name	Default Value	Required	Description
			exclude from the rollback process.
Preparatory SQL	no default	optional	File name that contains SQL statements that must be run before the database catalog update. This file is passed directly to SQLPlus and must be formatted as such. If not found on the target, it is downloaded from the software repository.
Run Database View Recompile	False	deprecated	If set to true, the Database View Recompile step will be run. Valid values are True and False.
Trust SSL Certificates	no default	deprecated	DMA no longer uses this workflow parameter to determine whether the workflow will trust any Secure Sockets Layer (SSL) certificate used to connect to the DMA web service. DMA uses the following parameter in the dma.xml file: <pre><Parameter name="com.hp.dma.conn.trustAllCertificates" values="VALUE" /></pre> Here, VALUE is true or false.
Web Service Password	no default	optional	Password for the DMA Discovery web service API.
Web Service URL	no default	optional	URL for the DMA Discovery web service API.
Web Service User	no default	optional	User who is capable of modifying the managed environment by using the DMA Discovery web service API.

Refreshing Database

Each workflow included in this solution pack has a set of **input parameters** whose values will be unique to your environment. If you provide correct values for the parameters that each scenario requires, the workflow will be able to accomplish its objective.

Tip: Input parameters are described in the "Parameters" topic for each workflow.

There are two steps required to customize this solution:

1. Ensure that all required parameters are visible. You do this by using the **workflow editor**.

To perform a simple database refresh, you can use the default values for most parameters. To use more advanced features of this solution, you will need to expose additional parameters.

2. Specify the values for those parameters. You do this when you create a **deployment**.

Note: Each of these steps is explained in greater detail in the "How to Use this Workflow" topic for each workflow.

The information presented here assumes the following:

- DMA is installed and operational.
- At least one suitable target server is available.
- You are logged in to the DMA web interface.
- You have permission to create, edit, and deploy copies of the workflows included in this solution pack.

Oracle - Extract Database via RMAN

This workflow performs a full database backup using Oracle Recovery Manager (RMAN) for the purpose of performing a database refresh. The RMAN backup set files can be stored in the local file system or on a network share.

RMAN stores an image of the database. It optimizes both speed and space consumption, and it performs block-level corruption detection during both the backup and restore phases of a database refresh.

Note: You cannot use this workflow to perform a cross-platform database refresh (for example: Linux to Solaris). You must use the Oracle Data Pump workflows included in this solution pack if you want to perform a cross-platform refresh.

To use this workflow in your environment, see the following information:

Topic	Information Included
"Prerequisites for this Workflow"	List of prerequisites that must be satisfied before you can run this workflow
"How this Workflow Works"	Information about what the workflow does, including validation checks performed, steps executed, and a high-level process flow
"How to Run this Workflow"	Instructions for running this workflow in your environment
"Sample Scenarios"	Examples of typical parameter values for this workflow
"Parameters for Oracle - Extract Database via RMAN"	List of input parameters for this workflow

Note: To view the steps included in this workflow, see the [Steps for Oracle - Extract Database via RMAN](#).

Prerequisites for this Workflow

Be sure that the following prerequisites are satisfied before you run the ["Oracle - Extract Database via RMAN"](#) workflow:

1. The DMA client must be installed on all target servers.
2. The Target Directory must exist prior to the execution of the workflow. This directory can be local, or it can be a Network File System (NFS) mount point.

Note: If you specify an NFS mount point, the pertinent NFS share must be available to the target server, and it must be mounted prior to running this workflow.

3. The specified Oracle Database user must have READ and WRITE permission for the specified Target Directory.
4. The Oracle Database software must be provisioned, and the database must exist in the target instance prior to workflow execution.

Note: For RMAN backup files, the destination database structure, database name, and Oracle SID must match that of the source.

For more information about prerequisites for Oracle Database, refer to the [Oracle Database Product Documentation](#).

How this Workflow Works

This topic contains the following information about the ["Oracle - Extract Database via RMAN"](#) workflow:

Overview

This workflow performs a full database backup using Oracle Recovery Manager (RMAN) for the purpose of performing a database refresh. You can instruct the workflow to store the RMAN backup set files in the local file system or on a network share.

You can use this workflow as part of a database refresh process. Database refresh involves moving the contents of a database in one Oracle instance into a database in another Oracle instance. This is useful, for example, if you want to move a database from a traditional IT infrastructure to a private cloud. It is also useful if you want to duplicate production data in a test environment for application development or troubleshooting purposes.

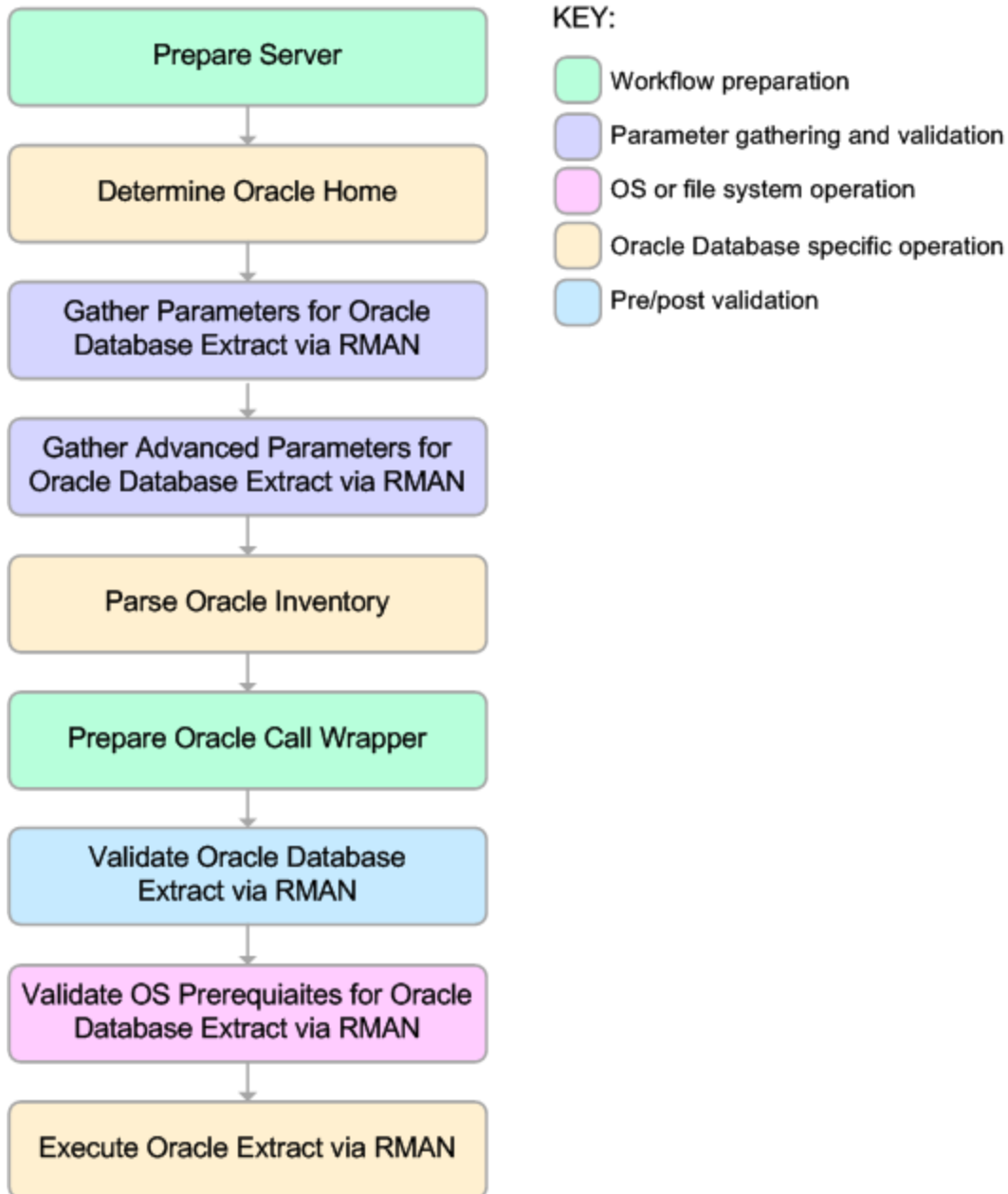
Validation Checks Performed

The workflow validates the following conditions:

1. The Oracle Home derived in the Determine Oracle Home step is a fully qualified path that exists on the target server.
2. The specified Target Directory exists, either locally or on a network share, and is writable.
3. The following system utilities are available: `ar`, `make`, `ls`, `nm`, `unzip`, and `mkdir`.
4. The workflow can connect to the Oracle SID derived in the Determine Oracle Home step.
5. All specified Ignorable Oracle Errors can safely be ignored.
6. The specified Tag Name parameter is not an empty string.
7. The specified Max Piece Size is at least 40 KByte and less than 16 TByte.

Steps Executed

The "Oracle - Extract Database via RMAN" workflow includes the following steps. Each step must complete successfully before the next step can start. If a step fails, the workflow reports a failure, and all subsequent steps are skipped.



Process Flow

This workflow performs the following tasks:

1. Determines the target server platform type, and identifies the server call wrapper.
2. Determines the Oracle Home path by reading the oratab file.
3. Gathers all required and optional parameters.
4. Determines the OS owner of the Oracle Home directory.
5. Prepares the instance call wrapper based on the specified Oracle User.
6. Validates all parameter values specified or derived.
7. Performs the RMAN backup.

How to Run this Workflow

The following instructions show you how to customize and run the ["Oracle - Extract Database via RMAN"](#) workflow in your environment.

The workflow provides default values for some parameters. These default values are usually sufficient for a "typical" installation. You can override the defaults by specifying parameter values in the deployment. You can also expose additional parameters in the workflow, if necessary, to accomplish more advanced scenarios. Any parameters not explicitly specified in the deployment will have the default values listed in ["Parameters for Oracle - Extract Database via RMAN" on page 382](#)

Note: Before following this procedure, review the ["Prerequisites for this Workflow"](#), and ensure that all requirements are satisfied.

To use the Oracle - Extract Database via RMAN workflow:

1. Create a deployable copy of the workflow.
2. Determine the values that you will specify for the following parameters: show

Parameter Name	Default Value	Required	Description
Oracle User	oracle	required	Oracle user that owns the ORACLE_HOME on the target Oracle database server. This user will perform the RMAN backup.
Target Directory	no default	required	Directory where the RMAN backup files will be placed. This directory must exist prior to workflow execution. The specified Oracle User must have READ and WRITE permissions for this directory. This directory must be accessible to the target database server.

Note: This is the minimum set of parameters required to run this workflow. You may need to expose additional parameters depending on your objectives.

See ["Parameters for Oracle - Extract Database via RMAN" on page 382](#) for detailed descriptions of all input parameters for this workflow, including default values.

3. In the workflow editor, expose any additional parameters that you need. You will specify values for those parameters when you create the deployment or at runtime.
4. Save the changes to the workflow (click **Save** in the lower right corner).
5. Create a new deployment.
6. On the Parameters tab, specify values (or set the type to Runtime Value) for the required parameters listed in step 2 and any additional parameters that you have exposed. You do not need

to specify values for those parameters whose default values are appropriate for your environment.

7. On the Targets tab, specify one or more targets for this deployment.
8. Save the deployment (click **Save** in the lower right corner).
9. Run the workflow using this deployment, specifying any runtime parameters.

To verify the results:

The workflow will complete and report SUCCESS on the Console if it has run successfully. If an error occurs during workflow execution, the error is logged, and the workflow terminates in the FAILURE state.

Sample Scenarios

This topic shows you how to use various parameters to achieve the following database backup scenarios in your environment using the ["Oracle - Extract Database via RMAN"](#) workflow:

Scenario 1: Create a Backup Set on the Local File System

This is the simplest RMAN extract scenario. In this example, the backup set is stored on the local file system. The parameters shown here are visible by default.

Parameter Name	Example Value	Description
Oracle User	oracle	Oracle user that owns the ORACLE_HOME on the target Oracle database server. This user will perform the RMAN backup.
Target Directory	/var/bckp/April2012/rman_04032012	Directory where the RMAN backup files will be placed. This directory must exist prior to workflow execution. The specified Oracle User must have READ and WRITE permissions for this directory. This directory must be accessible to the target database server.

Be sure that the default values for all remaining parameters are appropriate for your environment (see ["Parameters for Oracle - Extract Database via RMAN"](#)).

Scenario 2: Create a Backup Set on a Network Share

In this example, the backup set is stored on a network share. The parameters shown here are visible by default.

Parameter Name	Example Value	Description
Oracle User	oracle	Oracle user that owns the ORACLE_HOME on the target Oracle database server. This user will perform the RMAN backup.
Target Directory	myfileservr.mycompany.com:/uo1/nfs_share	Directory where the RMAN backup files will be placed. This directory must exist prior to workflow execution. The specified Oracle User must have READ and WRITE permissions for this directory. This directory must be accessible to the target database server.

Be sure that the default values for all remaining parameters are appropriate for your environment (see ["Parameters for Oracle - Extract Database via RMAN"](#)).

Scenario 3: Create a Backup Set Using Non-Default Parameters

In this example, the backup set is stored on the local file system. The first two parameters listed are visible by default; the remaining parameters must be exposed in the workflow so that they are available in the deployment.

Parameter Name	Example Value	Description
Oracle User	oracle	Oracle user that owns the ORACLE_HOME on the target Oracle database server. This user will perform the RMAN backup.
Target Directory	/var/bckp/April2012/rman_04032012	Directory where the RMAN backup files will be placed. This directory must exist prior to workflow execution. The specified Oracle User must have READ and WRITE permissions for this directory. This directory must be accessible to the target database server.
Ignorable Oracle Errors	ORA-39083, ORA-00959, ORA-01917, ORA-01918, ORA-01435	Comma delimited list of Oracle errors to ignore while executing the RMAN backup. The workflow always ignores ORA-39083, ORA-00959, ORA-01917, ORA-01918, ORA-01435, ORA-00942, ORA-31693, and ORA-20000. The workflow generates a warning but does not fail if it encounters LRM-00101, ORA-39000, ORA-31640, ORA-27037, ORA-31641, or ORA-27038.
Max Piece Size	2G	Maximum size (in MB) of an RMAN backup set piece (physical file).
Tag Name	FULL DATABASE BACKUP, FULLDB-BACKUP, ARCHIVED LOGS BACKUP, DMA REFRESH	A text string assigned to this backup.
Temporary File Location	/var/temp/rman_temp_files	Location to store temporary files while the workflow is running.

Be sure that the default values for all remaining parameters are appropriate for your environment (see ["Parameters for Oracle - Extract Database via RMAN"](#)).

Parameters for Oracle - Extract Database via RMAN

The following tables describe the required and optional input parameters for this workflow. Some of these parameters may not be initially visible in a deployment. For some parameters, if you do not specify a value for a parameter, a default value is assigned.

Parameters whose values are derived in one step and consumed by another step are not shown here.

Parameters Defined in this Step: Gather Parameters for Oracle Database Extract via RMAN

Parameter Name	Default Value	Required	Description
Oracle User	oracle	required	Oracle user that owns the ORACLE_HOME on the target Oracle database server. This user will perform the RMAN backup.
Target Directory	no default	required	Directory where the RMAN backup files will be placed. This directory must exist prior to workflow execution. The specified Oracle User must have READ and WRITE permissions for this directory. This directory must be accessible to the target database server.

Additional Parameters Defined in this Step: Gather Advanced Parameters for Oracle Database Extract via RMAN

Parameter Name	Default Value	Required	Description
Ignorable Oracle Errors	ORA-31684,ORA-39111,ORA-39151,ORA-31685,ORA-00001,RMAN-00571,RMAN-00569,RMAN-03002,RMAN-06054	optional	Comma delimited list of Oracle errors to ignore while executing the RMAN backup. The workflow always ignores ORA-39083, ORA-00959,ORA-01917,ORA-01918,ORA-01435,ORA-00942,ORA-31693, and ORA-20000. The workflow generates a warning but does not fail if it encounters LRM-00101, ORA-39000, ORA-31640, ORA-27037, ORA-31641, or ORA-27038.
Max Piece Size	1048576	optional	Maximum size (in MB) of an RMAN backup set piece (physical file).
Tag Name	DMA Refresh	optional	A text string assigned to this backup.
Temporary File Location	no default	optional	Location to store temporary files while the workflow is running.

Additional Parameter Defined in this Step: Parse Oracle Inventory

Parameter Name	Default Value	Required	Description
Inventory Files	see description	optional	Comma separated list of Oracle inventory file names (with absolute paths). If not specified, set to the appropriate default value for the target server operating system. Defaults are:

Additional Parameter Defined in this Step: Parse Oracle Inventory, continued

Parameter Name	Default Value	Required	Description
			Solaris: /var/opt/oracle/oraInst.loc Linux: /etc/oraInst.loc Windows: %ProgramFiles%\Oracle\Inventory

Oracle - Refresh Database via RMAN

This workflow restores an Oracle database from a previously created RMAN backup set. The backup set files can be located in the local file system or on a network share.

Note: You cannot use this workflow to perform a cross-platform database refresh (for example: Linux to Solaris). You must use the Oracle Data Pump workflows included in this solution pack if you want to perform a cross-platform refresh.

To use this workflow in your environment, see the following information:

Topic	Information Included
"Prerequisites for this Workflow"	List of prerequisites that must be satisfied before you can run this workflow
"How this Workflow Works"	Information about what the workflow does, including validation checks performed, steps executed, and a high-level process flow
"How to Run this Workflow"	Instructions for running this workflow in your environment
"Sample Scenarios"	Examples of typical parameter values for this workflow
"Parameters for Oracle - Refresh Database via RMAN"	List of input parameters for this workflow

Note: To view the steps included in this workflow, see the [Steps for Oracle - Refresh Database via RMAN](#).

Prerequisites for this Workflow

Be sure that the following prerequisites are satisfied before you run the ["Oracle - Refresh Database via RMAN"](#) workflow:

1. The DMA client must be installed on all target servers.
2. The Target Directory must exist prior to the execution of the workflow. This directory can be local, or it can be a Network File System (NFS) mount point.

Note: If you specify an NFS mount point, the pertinent NFS share must be available to the target server, and it must be mounted prior to running this workflow.

3. The specified Oracle Database user must have READ and WRITE permission for the specified Target Directory.
4. The Oracle Database software must be provisioned, and the database must exist in the target instance prior to workflow execution.

Note: For RMAN backup files, the destination database structure, database name, and Oracle SID must match that of the source.

For more information about prerequisites for Oracle Database, refer to the [Oracle Database Product Documentation](#).

How this Workflow Works

This topic contains the following information about the "Oracle - Refresh Database via RMAN" workflow:

Overview

This workflow performs a full RMAN database restore from a previously created RMAN backup set. A backup set contains an image that incorporates data from the following sources:

- Data files
- Archived redo log files
- Control files
- Server parameter files

The backup set can be located in the local file system or on a network share.

You can use this workflow as part of a database refresh process. Database refresh involves moving the contents of a database in one Oracle instance into a database in another Oracle instance. This is useful, for example, if you want to move a database from a traditional IT infrastructure to a private cloud. It is also useful if you want to duplicate production data in a test environment for application development or troubleshooting purposes.

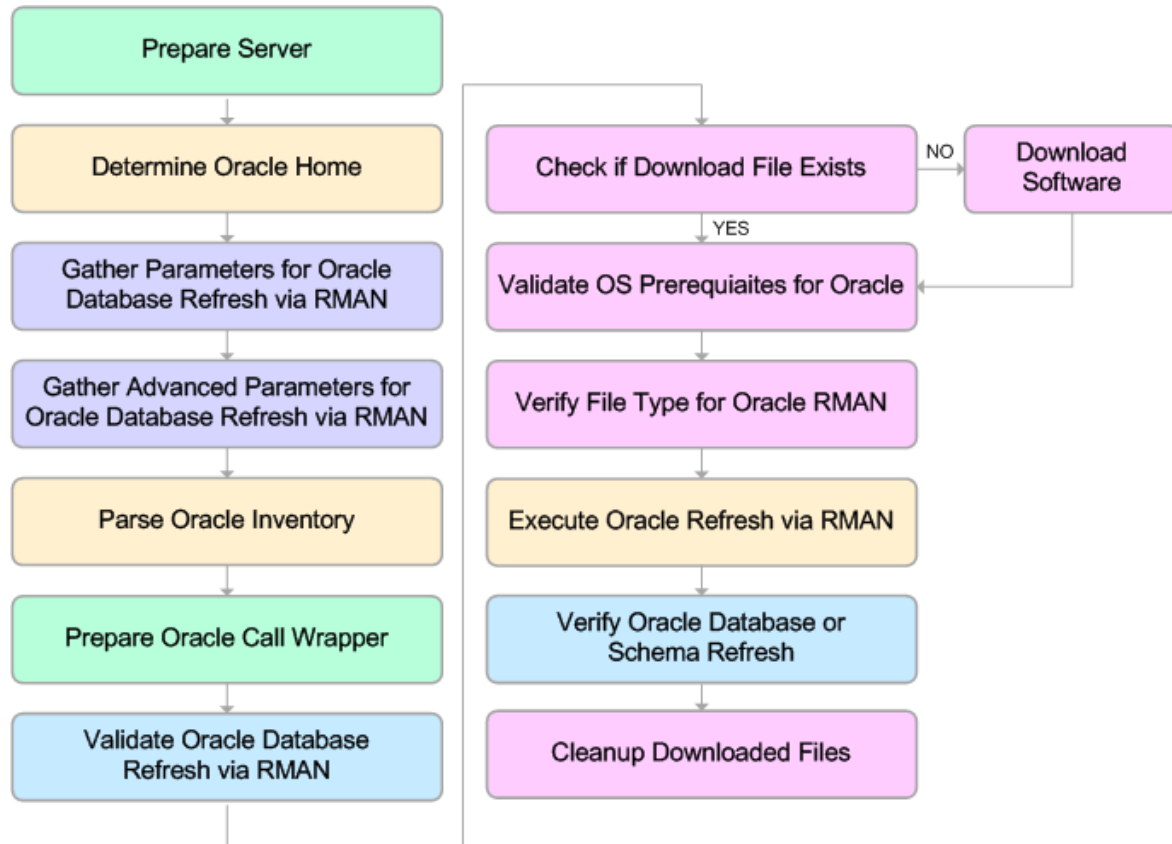
Validation Checks Performed

The workflow validates the following conditions:

1. The database to be restored is shut down.
2. The specified Target Directory exists, either locally or on a network share, and is writable.
3. The following system utilities are available: `ar`, `make`, `ls`, `nm`, `unzip`, and `mkdir`.
4. The specified Oracle Home exists and is, in fact, an Oracle home.
5. The workflow can connect to the specified Oracle SID in the specified Oracle Home.
6. The specified RMAN Archive Logs, RMAN Control File, and RMAN Data Files exist and have the proper format.
7. All specified Ignorable Oracle Errors can safely be ignored.
8. If a Verification SQL Script is specified, both that file and the Verification Result file exist.
9. The OS platform and Oracle Database version are supported by DMA.
10. Sufficient disk space is available to perform the database restore.

Steps Executed

The "Oracle - Refresh Database via RMAN" workflow includes the following steps. Each step must complete successfully before the next step can start. If a step fails, the workflow reports a failure, and all subsequent steps are skipped.



KEY:

- Workflow preparation
- Parameter gathering and validation
- OS or file system operation
- Oracle Database specific operation
- Pre/post validation

Process Flow

This workflow performs the following tasks:

1. Determines the target server platform type, and identifies the server call wrapper.
2. Gathers all required and optional parameters.
3. Determines the OS owner of the Oracle Home directory.
4. Prepares the instance call wrapper based on the specified Oracle Account.
5. Validates all parameter values specified or derived.
6. Determines whether the RMAN backup set files already exist on the target server. If the files do not yet exist, the workflow downloads them from the software repository.
7. Determines whether sufficient disk space is available to restore the database from the backup set.
8. Verifies that the specified backup set files constitute a valid RMAN backup set.
9. Performs the RMAN restore.
10. Verifies that the database was successfully restored by ensuring that the following conditions are true:
 - The database is accessible.
 - Temporary tablespace has been created.
 - No tablespaces are in backup mode.
11. Runs the Verification SQL Script (if specified), and compares the result to the specified Verification Result file.
12. Removes any files downloaded to facilitate this restore.

Sample Scenarios

This topic shows you how to use various parameters to achieve the following database backup scenarios in your environment using the ["Oracle - Refresh Database via RMAN"](#) workflow:

Scenario 1: Restore from a Backup Set on the Local File System

This is the simplest RMAN refresh scenario. In this example, the backup set is downloaded to the local file system. The parameters shown here are visible by default.

In this scenario, the Refresh Oracle Database via RMAN workflow uses extracted files from an RMAN backup. These are files that were generated by using the Extract Oracle Database via RMAN workflow or by using the RMAN backup utility. The Database ID parameter represents the Database Identification of the source Oracle database.

The workflow has additional input parameters that can be exposed and specified as needed. For example, you may want to use an encrypted RMAN backup file or increase the number of channels to speed up the refresh process.

Parameter Name	Example Value	Description
Oracle Account	oracle	The ORACLE_HOME to use if more than one home is found in the inventory file (or files).
RMAN Archive Logs	/var/tmp/rman_dump/ my_archivelog.bak	Archived redo log files that were generated from the source database. These redo logs are applied as part of the RMAN restore. Separate multiple files with commas. Include the full path where each file is located. For example: /home/oracle/DbRefresh/RMAN/ archivelog_DB2_04n11fnh.bak
RMAN Control File	/var/tmp/rman_dump/ my_controlfile.ora	Control File generated from the source database.
RMAN Data Files	/var/tmp/rman_dump/ my_datafile.bkp	RMAN backup data files created from the source database where the RMAN backup was performed. Separate multiple files with commas.
Target Directory	/var/tmp/rman_dump	Directory on the target database server where the RMAN backup files will be downloaded. This directory must exist prior to workflow execution. The Oracle Account user must have READ and WRITE access to this directory.
Database ID	1935744575	Database ID of the source database used to create the RMAN backup files.

Be sure that the default values for all remaining parameters are appropriate for your environment (see [Parameters for Oracle - Refresh Database via RMAN](#)).

Scenario 2: Restore from a Backup Set on a Network Share

In this example, the backup set is downloaded to a network share. Restoring from a backup set stored on a network share alleviates the need to transfer files onto the target database servers.

The parameters shown here are visible by default. The workflow has additional parameters that can be modified to best fit any particular refresh scenario. For example, you can specify encryption parameters, ignore errors generated by the Oracle RMAN utility that do not affect the database refresh, or turn on and tune additional channels to speed up the refresh process.

Parameter Name	Example Value	Description
Oracle Account	oracle	The ORACLE_HOME to use if more than one home is found in the inventory file (or files).
RMAN Archive Logs	/var/tmp/rman_dump/ my_archive.log.bak	Archived redo log files that were generated from the source database. These redo logs are applied as part of the RMAN restore. Separate multiple files with commas. Include the full path where each file is located. For example: /home/oracle/DbRefresh/RMAN/ archivelog_DB2_04n1lfnh.bak
RMAN Control File	/var/tmp/rman_dump/ my_controlfile.ora	Control File generated from the source database.
RMAN Data Files	/var/tmp/rman_dump/ my_datafile.bkp	RMAN backup data files created from the source database where the RMAN backup was performed. Separate multiple files with commas.
Target Directory	myfileservr.mycompany.com: /uo1/nfs_share	Directory on the target database server where the RMAN backup files will be downloaded. This directory must exist prior to workflow execution. The Oracle Account user must have READ and WRITE access to this directory.
Database ID	1935744575	Database ID of the source database used to create the RMAN backup files.

Be sure that the default values for all remaining parameters are appropriate for your environment (see Parameters for Oracle - Refresh Database via RMAN).

How to Run this Workflow

The following instructions show you how to customize and run the ["Oracle - Refresh Database via RMAN"](#) workflow in your environment.

The workflow provides default values for some parameters. These default values are usually sufficient for a "typical" installation. You can override the defaults by specifying parameter values in the deployment. You can also expose additional parameters in the workflow, if necessary, to accomplish more advanced scenarios. Any parameters not explicitly specified in the deployment will have the default values listed in ["Parameters for Oracle - Refresh Database via RMAN" on page 393](#)

Note: Before following this procedure, review the ["Prerequisites for this Workflow"](#), and ensure that all requirements are satisfied.

To use the Oracle - Refresh Database via RMAN workflow:

1. Create a deployable copy of the workflow.
2. Determine the values that you will specify for the following parameters:

Parameter Name	Default Value	Required	Description
Oracle Account	oracle	optional	Oracle user that owns the ORACLE_HOME on the target Oracle database server where the RMAN backup will be restored. This user will perform the RMAN restore. Required if inventory does not exist. Leave blank for windows.
RMAN Archive Logs	no default	required	Archived redo log files that were generated from the source database. These redo logs are applied as part of the RMAN restore. Separate multiple files with commas. Include the full path where each file is located. For example: /home/oracle/DbRefresh/RMAN/archive_log_DB2_04n11fnh.bak
RMAN Control File	no default	required	Control File generated from the source database.
RMAN Data Files	no default	required	RMAN backup data files created from the source database where the RMAN backup was performed. Separate multiple files with commas.
Target Directory	no default	required	Directory on the target database server where the RMAN backup files will be downloaded. This directory must exist prior to workflow execution. The Oracle Account user must have READ and WRITE access to this directory.
Database ID	no default	required	Database ID of the source database used to create the RMAN backup files.

Note: This is the minimum set of parameters required to run this workflow. You may need to expose additional parameters depending on your objectives.

See ["Parameters for Oracle - Refresh Database via RMAN" on the next page](#) for detailed descriptions of all input parameters for this workflow, including default values.

3. In the workflow editor, expose any additional parameters that you need. You will specify values for those parameters when you create the deployment or at runtime.
4. Save the changes to the workflow (click **Save** in the lower right corner).
5. Create a new deployment.
6. On the Parameters tab, specify values (or set the type to Runtime Value) for the required parameters listed in step 2 and any additional parameters that you have exposed. You do not need to specify values for those parameters whose default values are appropriate for your environment.
7. On the Targets tab, specify one or more targets for this deployment.
8. Save the deployment (click **Save** in the lower right corner).
9. Run the workflow using this deployment, specifying any runtime parameters.

To verify the results:

The workflow will complete and report SUCCESS on the Console if it has run successfully. If an error occurs during workflow execution, the error is logged, and the workflow terminates in the FAILURE state.

Parameters for Oracle - Refresh Database via RMAN

The following tables describe the required and optional input parameters for this workflow. Some of these parameters may not be initially visible in a deployment. For some parameters, if you do not specify a value for a parameter, a default value is assigned.

Parameters whose values are derived in one step and consumed by another step are not shown here.

Parameters Defined in this Step: Gather Parameters for Oracle Database Refresh via RMAN

Parameter Name	Default Value	Required	Description
Inventory Files	see description	optional	Comma separated list of Oracle inventory file names (with absolute paths). If not specified, set to the appropriate default value for the target server operating system. Defaults are: Solaris: /var/opt/oracle/oraInst.loc Linux: /etc/oraInst.loc Windows: %ProgramFiles%\Oracle\Inventory
Oracle Account	oracle	optional	Oracle user that owns the ORACLE_HOME on the target Oracle database server where the RMAN backup will be restored. This user will perform the RMAN restore. Required if inventory does not exist. Leave blank for windows.
Oracle Home	no default	optional	The ORACLE_HOME to use if more than one home is found in the inventory file (or files).
Oracle SID	no default	required	The Oracle System ID (SID) of the target database.
RMAN Archive Logs	no default	required	Archived redo log files that were generated from the source database. These redo logs are applied as part of the RMAN restore. Separate multiple files with commas. Include the full path where each file is located. For example: /home/oracle/DbRefresh/RMAN/ archivelog_DB2_04n11fnh.bak
RMAN Control File	no default	required	Control File generated from the source database.
RMAN Data Files	no default	required	RMAN backup data files created from the source database where the RMAN backup was performed. Separate multiple files with commas.
Target Directory	no default	required	Directory on the target database server where the RMAN backup files will be downloaded. This directory must exist prior to workflow execution. The Oracle Account user must have READ and WRITE access to this directory.

Additional Parameters Defined in this Step: Gather Advanced Parameters for Oracle Database Refresh via RMAN

Parameter Name	Default Value	Required	Description
Ignorable Oracle Errors	ORA-31684,ORA-39111,ORA-39151,ORA-31685,ORA-00001,RMAN-06497,RMAN-00571,RMAN-00569,RMAN-03002,RMAN-06054	optional	<p>Comma delimited list of Oracle errors to ignore while executing the RMAN restore.</p> <p>The workflow always ignores ORA-39083, ORA-00959,ORA-01917,ORA-01918,ORA-01435,ORA-00942,ORA-31693, and ORA-20000.</p> <p>The workflow generates a warning but does not fail if it encounters LRM-00101, ORA-39000, ORA-31640, ORA-27037, ORA-31641, or ORA-27038.</p>
Verification Result	no default	optional	<p>Name (with absolute path) of a text file containing the expected results of the SQL queries included in the Verification SQL Script.</p> <p>This parameter is required if you provide a Verification SQL Script. Be sure to run the Verification SQL Script on the SOURCE database before running this workflow, and copy the results into this file.</p> <p>You must provide this file in a location where the workflow can access it.</p>
Verification SQL Script	no default	optional	<p>Name (with absolute path) of a text file containing a SQL script that verifies the following:</p> <ul style="list-style-type: none"> • The import operation was successful. • No data is missing. <p>You must provide this file in a location where the workflow can access it. The expected results of the queries included in this script must be provided in the Verification Result file.</p>

Additional Parameters Defined in this Step: Verify File Type for Oracle RMAN

Parameter Name	Default Value	Required	Description
RMAN Tags	FULL DATABASE BACKUP,FULLDB-BACKUP,ARCHIVED LOGS BACKUP,DMA REFRESH	optional	<p>Tags to search for in the specified RMAN backup files. Separate multiple tags with commas.</p> <p>You can assign a tag when you perform an RMAN backup on the source database (see "Oracle - Extract Database via RMAN" on page 373).</p>

Additional Parameters Defined in this Step: Execute Oracle Refresh via RMAN

Parameter Name	Default Value	Required	Description
Database ID	no default	required	Database ID of the source database used to create the RMAN backup files.

Oracle - Extract and Refresh Database via RMAN

This workflow performs a database refresh using Oracle Recovery Manager (RMAN) to first perform a full database backup on the SOURCE database and then perform a full database restore on the DESTINATION database.

RMAN stores an image of the database. It optimizes both speed and space consumption, and it performs block-level corruption detection during both the backup and restore phases of a database refresh.

Note: You cannot use this workflow to perform a cross-platform database refresh (for example: Linux to Solaris). You must use the Oracle Data Pump workflows included in this solution pack if you want to perform a cross-platform refresh.

To use this workflow in your environment, see the following information:

Topic	Information Included
"Prerequisites for this Workflow"	List of prerequisites that must be satisfied before you can run this workflow
"How this Workflow Works"	Information about what the workflow does, including validation checks performed, steps executed, and a high-level process flow
"How to Run this Workflow"	Instructions for running this workflow in your environment
"Sample Scenarios"	Examples of typical parameter values for this workflow
"Parameters for Oracle - Extract and Refresh Database via RMAN"	List of input parameters for this workflow

Note: To view the steps included in this workflow, see the [Steps for Oracle - Extract and Refresh Database via RMAN](#).

Prerequisites for this Workflow

Be sure that the following prerequisites are satisfied before you run the ["Oracle - Extract and Refresh Database via RMAN"](#) workflow:

1. The DMA client must be installed on all target servers.
2. The Target Directory must exist prior to the execution of the workflow. This directory can be local, or it can be a Network File System (NFS) mount point.

Note: If you specify an NFS mount point, the pertinent NFS share must be available to the target server, and it must be mounted prior to running this workflow.

3. The specified Oracle Database user must have READ and WRITE permission for the specified Target Directory.
4. The Oracle Database software must be provisioned, and the database must exist in the target instance prior to workflow execution.

For more information about prerequisites for Oracle Database, refer to the [Oracle Database Product Documentation](#).

How this Workflow Works

This topic contains the following information about the "Oracle - Extract and Refresh Database via RMAN" workflow:

Overview

This workflow performs a database refresh using Oracle Recovery Manager (RMAN) to first perform a full database backup on the SOURCE database and then perform a full database restore on the DESTINATION database.

RMAN stores an image of the database. It optimizes both speed and space consumption, and it performs block-level corruption detection during both the backup and restore phases of a database refresh.

Note: You cannot use this workflow to perform a cross-platform database refresh (for example: Linux to Solaris). You must use the Oracle Data Pump workflows included in this solution pack if you want to perform a cross-platform refresh.

Validation Checks Performed

The workflow first validates the following conditions for the SOURCE database:

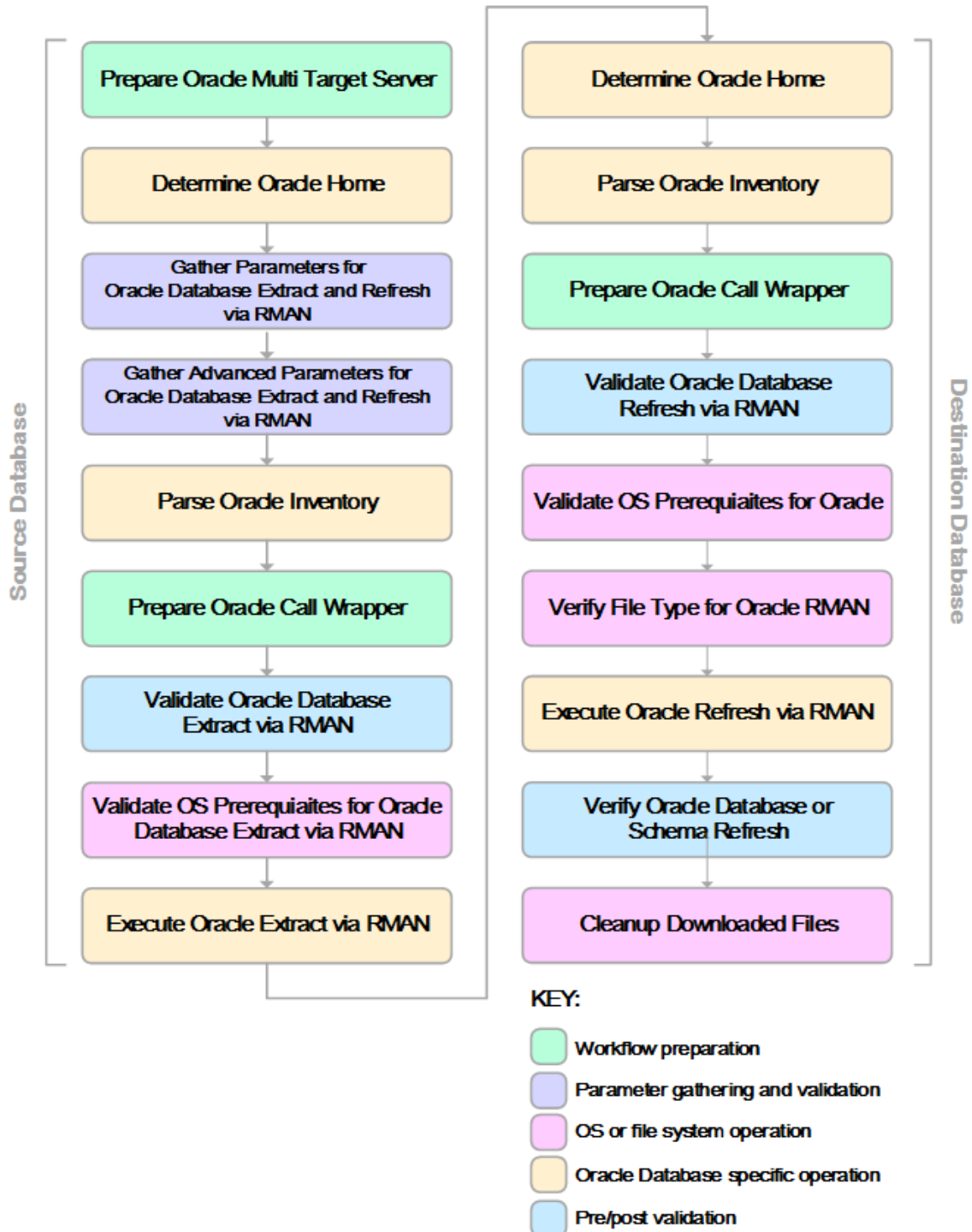
1. The Oracle Home derived in the Determine Oracle Home step is a fully qualified path that exists on the target server.
2. The specified Target Directory exists, either locally or on a network share, and is writable.
3. The following system utilities are available: `ar`, `make`, `ls`, `nm`, `unzip`, and `mkdir`.
4. The workflow can connect to the Oracle SID derived in the Determine Oracle Home step.
5. All specified Ignorable Oracle Errors can safely be ignored.
6. The specified Tag Name parameter is not an empty string.
7. The specified Max Piece Size is at least 40 KByte and less than 16 TByte.

The workflow validates the following conditions for the DESTINATION database:

1. The database to be restored is shut down.
2. The specified Target Directory exists, either locally or on a network share, and is writable.
3. The following system utilities are available: `ar`, `make`, `ls`, `nm`, `unzip`, and `mkdir`.
4. The specified Oracle Home exists and is, in fact, an Oracle home.
5. The workflow can connect to the specified Oracle SID in the specified Oracle Home.
6. The specified RMAN Archive Logs, RMAN Control File, and RMAN Data Files exist and have the proper format.
7. All specified Ignorable Oracle Errors can safely be ignored.
8. If a Verification SQL Script is specified, both that file and the Verification Result file exist.
9. The OS platform and Oracle Database version are supported by DMA.
10. Sufficient disk space is available to perform the database restore.

Steps Executed

The "Oracle - Extract and Refresh Database via RMAN" workflow includes the following steps. Each step must complete successfully before the next step can start. If a step fails, the workflow reports a failure, and all subsequent steps are skipped.



Process Flow

This workflow first performs the following tasks on the SOURCE database:

1. Determines the target server platform type, and identifies the server call wrapper.
2. Determines the Oracle Home path by reading the oratab file.
3. Gathers all required and optional parameters.
4. Determines the OS owner of the Oracle Home directory.
5. Prepares the instance call wrapper based on the specified Oracle User.
6. Validates all parameter values specified or derived.
7. Performs the RMAN backup.

The workflow then performs the following tasks on the DESTINATION database:

1. Determines the OS owner of the Oracle Home directory.
2. Prepares the instance call wrapper based on the specified Oracle Account.
3. Validates all parameter values specified or derived.
4. Determines whether the RMAN backup set files already exist on the target server. If the files do not yet exist, the workflow downloads them from the software repository.
5. Determines whether sufficient disk space is available to restore the database from the backup set.
6. Verifies that the specified backup set files constitute a valid RMAN backup set.
7. Performs the RMAN restore.
8. Verifies that the database was successfully restored by ensuring that the following conditions are true:
 - The database is accessible.
 - Temporary tablespace has been created.
 - No tablespaces are in backup mode.
9. Runs the Verification SQL Script (if specified), and compares the result to the specified Verification Result file.
10. Removes any files downloaded to facilitate this restore.

How to Run this Workflow

The following instructions show you how to customize and run the ["Oracle - Extract and Refresh Database via RMAN"](#) workflow in your environment.

The workflow provides default values for some parameters. These default values are usually sufficient for a "typical" installation. You can override the defaults by specifying parameter values in the deployment. You can also expose additional parameters in the workflow, if necessary, to accomplish more advanced scenarios. Any parameters not explicitly specified in the deployment will have the default values listed in ["Parameters for Oracle - Extract and Refresh Database via RMAN" on page 408](#)

Note: Before following this procedure, review the ["Prerequisites for this Workflow"](#), and ensure that all requirements are satisfied.

To use the Oracle - Extract and Refresh Database via RMAN workflow:

1. Create a deployable copy of the workflow.
2. Determine the values that you will specify for the following parameters: show

Parameter Name	Default Value	Required	Description
ALL - Target Directory	no default	required	Directory where the RMAN backup files will be placed on the SOURCE database server and subsequently downloaded on DESTINATION database server. This directory must be the same on both the SOURCE and DESTINATION servers. The directory must exist on both servers before the workflow runs, and it must be accessible to the Oracle Account user.
EXPORT - Oracle User	no default	required	Oracle user that owns the ORACLE_HOME on the SOURCE Oracle database server. This user will perform the RMAN backup.
IMPORT - Oracle Account	no default	optional	Oracle user that owns the ORACLE_HOME on the DESTINATION database server. This user will perform the RMAN restore.

Note: This is the minimum set of parameters required to run this workflow. You may need to expose additional parameters depending on your objectives.

See ["Parameters for Oracle - Extract and Refresh Database via RMAN" on page 408](#) for detailed descriptions of all input parameters for this workflow, including default values.

3. In the workflow editor, expose any additional parameters that you need. You will specify values for these parameters when you create the deployment.
4. Save the changes to the workflow (click **Save** in the lower right corner).

5. Create a new deployment.
 - a. On the Targets tab, select all the target servers—both source and destination—that will participate in this database refresh. The targets that you select here will be available in the Target Parameters drop-down menus on the Run page (see [step 7](#)).
 - b. On the Parameters tab, specify values for the required parameters listed in [step 2](#) and any additional parameters that you exposed in [step 3](#). You do not need to specify values for those parameters whose default values are appropriate for your environment.
6. Save the deployment (click **Save** in the lower right corner).
7. Run the workflow using this deployment.

On the Run page, select the following targets from the respective drop-down menus:

Parameter Name	Default	Description
Source	no default	Instance that contains the database whose contents will be extracted.
Destination	no default	Instance where the database will be restored.

To verify the results:

The workflow will complete and report SUCCESS on the Console if it has run successfully. If an error occurs during workflow execution, the error is logged, and the workflow terminates in the FAILURE state.

Sample Scenarios

This topic shows you how to use various parameters to achieve the following database backup scenarios in your environment using the ["Oracle - Extract and Refresh Database via RMAN"](#) workflow:

Scenario 1: Store the Backup Set on the Local File System

This is the simplest RMAN extract and refresh scenario. In this example, the backup set is stored on the local file system of the SOURCE database server. The backup set files are then downloaded to the same location in the local file system of the DESTINATION database server. The parameters shown here are visible by default.

Parameter Name	Example Value	Description
ALL - Target Directory	/var/bckp/April2012/ rman_04032012	Directory where the RMAN backup files will be placed on the SOURCE database server and subsequently downloaded on DESTINATION database server. This directory must be the same on both the SOURCE and DESTINATION servers. The directory must exist on both servers before the workflow runs, and it must be accessible to the Oracle Account user.
EXPORT - Oracle User	oracle	Oracle user that owns the ORACLE_HOME on the SOURCE Oracle database server. This user will perform the RMAN backup.
IMPORT - Oracle Account	oracle	Oracle user that owns the ORACLE_HOME on the DESTINATION database server. This user will perform the RMAN restore.

Be sure that the default values for all remaining parameters are appropriate for your environment (see ["Parameters for Oracle - Extract and Refresh Database via RMAN"](#)).

Scenario 2: Store the Backup Set on a Network Share

In this example, the backup set is stored on a network share that both the SOURCE and DESTINATION database servers can access. The parameters shown here are visible by default.

Parameter Name	Example Value	Description
ALL - Target Directory	myfileservier.mycompany.com:/uo1/nfs_share	Directory where the RMAN backup files will be placed on the SOURCE database server and subsequently downloaded on DESTINATION database server. This directory must be the same on both the SOURCE and DESTINATION servers. The directory must exist on both servers before the workflow runs, and it must be accessible to the Oracle Account user.
EXPORT - Oracle User	oracle	Oracle user that owns the ORACLE_HOME on the SOURCE Oracle database server. This user will perform the RMAN backup.
IMPORT - Oracle Account	oracle	Oracle user that owns the ORACLE_HOME on the DESTINATION database server. This user will perform the RMAN restore.

Be sure that the default values for all remaining parameters are appropriate for your environment (see ["Parameters for Oracle - Extract and Refresh Database via RMAN"](#)).

Scenario 3: Create a Backup Set Using Non-Default Parameters

In this example, the backup set is stored on the local file systems. The first two parameters listed are visible by default; the remaining parameters must be exposed in the workflow so that they are available in the deployment.

Parameter Name	Example Value	Description
ALL - Target Directory	myfileservr.mycompany.com: /uo1/nfs_share	Directory where the RMAN backup files will be placed on the SOURCE database server and subsequently downloaded on DESTINATION database server. This directory must be the same on both the SOURCE and DESTINATION servers. The directory must exist on both servers before the workflow runs, and it must be accessible to the Oracle Account user.
EXPORT - Oracle User	oracle	Oracle user that owns the ORACLE_HOME on the SOURCE Oracle database server. This user will perform the RMAN backup.
IMPORT - Oracle Account	oracle	Oracle user that owns the ORACLE_HOME on the DESTINATION database server. This user will perform the RMAN restore.
ALL - Ignorable Oracle Errors	ORA-39083, ORA-00959, ORA-01917, ORA-01918, ORA-01435	Comma delimited list of Oracle errors to ignore while executing the RMAN extract and restore operations. The workflow always ignores ORA-39083, ORA-00959, ORA-01917, ORA-01918, ORA-01435, ORA-00942, ORA-31693, and ORA-20000. The workflow generates a warning but does not fail if it encounters LRM-00101, ORA-39000, ORA-31640, ORA-27037, ORA-31641, or ORA-27038.
EXPORT - Max Piece Size	524288	Maximum size (in MB) of an RMAN backup set piece (physical file).
EXPORT - Tag Name	FULL DATABASE BACKUP, FULLDB-BACKUP, ARCHIVED LOGS BACKUP, DMA REFRESH	A text string assigned to this backup.
EXPORT - Temporary File Location	/var/temp/ rman_temp_files	Location to store temporary files while the workflow is running.
IMPORT - Verification Result	/var/temp/ dbrefresh_ver_result.xml	Name (with absolute path) of a text file containing the expected results of the SQL queries included in the Verification SQL Script. This parameter is required if you provide a Verification SQL Script. Be sure to run the Verification SQL Script on the SOURCE database

Parameter Name	Example Value	Description
		<p>before running this workflow, and copy the results into this file.</p> <p>You must provide this file in a location where the workflow can access it.</p>
IMPORT - Verification SQL Script	/var/temp/dbrefresh_ver.sql	<p>Name (with absolute path) of a text file containing a SQL script that verifies the following:</p> <ul style="list-style-type: none"> • The import operation on the DESTINATION database server was successful. • No data is missing. <p>You must provide this file in a location where the workflow can access it. The expected results of the queries included in this script must be provided in the Verification Result file.</p>

Be sure that the default values for all remaining parameters are appropriate for your environment (see ["Parameters for Oracle - Extract and Refresh Database via RMAN"](#)).

Parameters for Oracle - Extract and Refresh Database via RMAN

The following tables describe the required and optional input parameters for this workflow. Some of these parameters may not be initially visible in a deployment. For some parameters, if you do not specify a value for a parameter, a default value is assigned.

Parameters whose values are derived in one step and consumed by another step are not shown here.

Parameters Defined in this Step: Gather Parameters for Oracle Database Extract and Refresh via RMAN

Parameter Name	Default Value	Required	Description
ALL - Target Directory	no default	required	Directory where the RMAN backup files will be placed on the SOURCE database server and subsequently downloaded on DESTINATION database server. This directory must be the same on both the SOURCE and DESTINATION servers. The directory must exist on both servers before the workflow runs, and it must be accessible to the Oracle Account user.
EXPORT - Inventory Files	see description	optional	Comma separated list of Oracle inventory file names (with absolute paths) on the SOURCE database server. Defaults are: Solaris: /var/opt/oracle/oraInst.loc Linux: /etc/oraInst.loc Windows: %ProgramFiles%\Oracle\Inventory
EXPORT - Oracle User	no default	required	Oracle user that owns the ORACLE_HOME on the SOURCE Oracle database server. This user will perform the RMAN backup.
EXPORT - Target Directory	no default	optional	Directory accessible to the SOURCE database server where the RMAN backup files will be saved. This directory must exist before the workflow runs. The Oracle Account user must have READ and WRITE permissions for this directory. This directory must be also be accessible to the DESTINATION database server.
IMPORT - Inventory Files	no default	optional	Comma separated list of Oracle inventory file names (with absolute paths) on the DESTINATION database server.
IMPORT - Oracle Account	no default	optional	Oracle user that owns the ORACLE_HOME on the DESTINATION database server. This user will perform the RMAN restore.
Server Wrapper	jython	required	Command that will be used to construct the call wrapper. The workflow uses the call wrapper to execute subsequent steps as either the OS administrative user or the Oracle user who owns the pertinent ORACLE_HOME. For example: sudo su - root /opt/hp/dma/client/bin/jython.sh sudo su - sysdba /opt/hp/dma/client/bin/jython.sh

Additional Parameters Defined in this Step: Gather Advanced Parameters for Oracle Database Extract and Refresh via RMAN

Parameter Name	Default Value	Required	Description
ALL - Ignorable Oracle Errors	ORA-31684,ORA-39111,ORA-39151,ORA-31685,ORA-00001,RMAN-06497,RMAN-00571,RMAN-00569,RMAN-03002,RMAN-06054	optional	<p>Comma delimited list of Oracle errors to ignore while executing the RMAN extract and restore operations.</p> <p>The workflow always ignores ORA-39083, ORA-00959,ORA-01917,ORA-01918,ORA-01435,ORA-00942,ORA-31693, and ORA-20000.</p> <p>The workflow generates a warning but does not fail if it encounters LRM-00101, ORA-39000, ORA-31640, ORA-27037, ORA-31641, or ORA-27038.</p>
EXPORT - Max Piece Size	1048576	optional	Maximum size (in MB) of an RMAN backup set piece (physical file).
EXPORT - Tag Name	DMA Refresh	optional	A text string assigned to this backup.
EXPORT - Temporary File Location	no default	optional	Location to store temporary files while the workflow is running.
IMPORT - Verification Result	no default	optional	<p>Name (with absolute path) of a text file containing the expected results of the SQL queries included in the Verification SQL Script.</p> <p>This parameter is required if you provide a Verification SQL Script. Be sure to run the Verification SQL Script on the SOURCE database before running this workflow, and copy the results into this file.</p> <p>You must provide this file in a location where the workflow can access it.</p>
IMPORT - Verification SQL Script	no default	optional	<p>Name (with absolute path) of a text file containing a SQL script that verifies the following:</p> <ul style="list-style-type: none"> The import operation on the DESTINATION database server was successful. No data is missing. <p>You must provide this file in a location where the workflow can access it. The expected results of the queries included in this script must be provided in the Verification Result file.</p>

Oracle - Export Database via Data Pump

This workflow performs a full database export using the Oracle Data Pump utility for the purpose of performing a database refresh. The Data Pump Export files can be stored in the local file system or on a network share. You can use this workflow to implement a cross-platform database refresh (for example: Linux to Solaris).

Data Pump uses SQL commands to import and export specific data objects. It is slower than the Oracle Recovery Manager (RMAN) but offers more flexibility.

The workflow automatically detects which ORACLE_HOME and ORACLE_SID to use when performing the Data Pump export. You can specify the encryption mode, compression level, and file size to use for the export—be sure to use the same settings for the subsequent import.

You have the option of providing a Data Pump parameter file or entering the parameters on the Deployment page. In either case, the parameter values are validated prior to the Data Pump export. If you do not provide a parameter file, the workflow creates one based on the parameter values that you specify on the Deployment page. If you do not specify a value for a particular parameter, the default value is used (see ["Parameters for Oracle - Export Database via Data Pump" on page 423](#)).

To use this workflow in your environment, see the following information:

Topic	Information Included
"Prerequisites for this Workflow"	List of prerequisites that must be satisfied before you can run this workflow
"How this Workflow Works"	Information about what the workflow does, including validation checks performed, steps executed, and a high-level process flow
"How to Run this Workflow"	Instructions for running this workflow in your environment
"Sample Scenarios"	Examples of typical parameter values for this workflow
"Parameters for Oracle - Export Database via Data Pump"	List of input parameters for this workflow

Note: The documentation for this workflow refers to the workflow and its steps by their base names. The names in the DMA user interface may have a version appended, for example, v2.

Note: To view the steps included in this workflow, see the [Steps for Oracle - Export Database via Data Pump](#).

Prerequisites for this Workflow

Be sure that the following prerequisites are satisfied before you run the ["Oracle - Export Database via Data Pump"](#) workflow:

1. The DMA client must be installed on all target servers.
2. The Target Directory must exist prior to the execution of the workflow. This directory can be local, or it can be a Network File System (NFS) mount point.

Note: If you specify an NFS mount point, the pertinent NFS share must be available to the target server, and it must be mounted prior to running this workflow.

3. The specified Oracle Database user must have READ and WRITE permission for the specified Target Directory.
4. The Oracle Database software must be provisioned, and the database must exist in the target instance prior to workflow execution.

Note: For Data Pump workflows, you must specify the same Content and Encryption Password settings for the export and any subsequent import operations.

For more information about prerequisites for Oracle Database, refer to the [Oracle Database Product Documentation](#).

How this Workflow Works

This topic contains the following information about the ["Oracle - Export Database via Data Pump"](#) workflow:

Overview

This workflow performs a full database export using the Oracle Data Pump utility for the purpose of performing a database refresh. The Data Pump Export files can be stored in the local file system or on a network share. You can use this workflow to implement a cross-platform database refresh (for example: Linux to Solaris).

Data Pump uses SQL commands to import and export specific data objects. It is slower than the Oracle Recovery Manager (RMAN) but offers more flexibility.

The workflow automatically detects which ORACLE_HOME and ORACLE_SID to use when performing the Data Pump export. You can specify the encryption mode, compression level, and file size to use for the export—be sure to use the same settings for the subsequent import.

You have the option of providing a Data Pump parameter file or entering the parameters on the Deployment page. In either case, the parameter values are validated prior to the Data Pump export. If you do not provide a parameter file, the workflow creates one based on the parameter values that you specify on the Deployment page. If you do not specify a value for a particular parameter, the default value is used (see ["Parameters for Oracle - Export Database via Data Pump" on page 423](#)).

You can use this workflow as part of a database refresh process. Database refresh involves moving the contents of a database in one Oracle instance into a database in another Oracle instance. This is useful, for example, if you want to move a database from a traditional IT infrastructure to a private cloud. It is also useful if you want to duplicate production data in a test environment for application development or troubleshooting purposes.

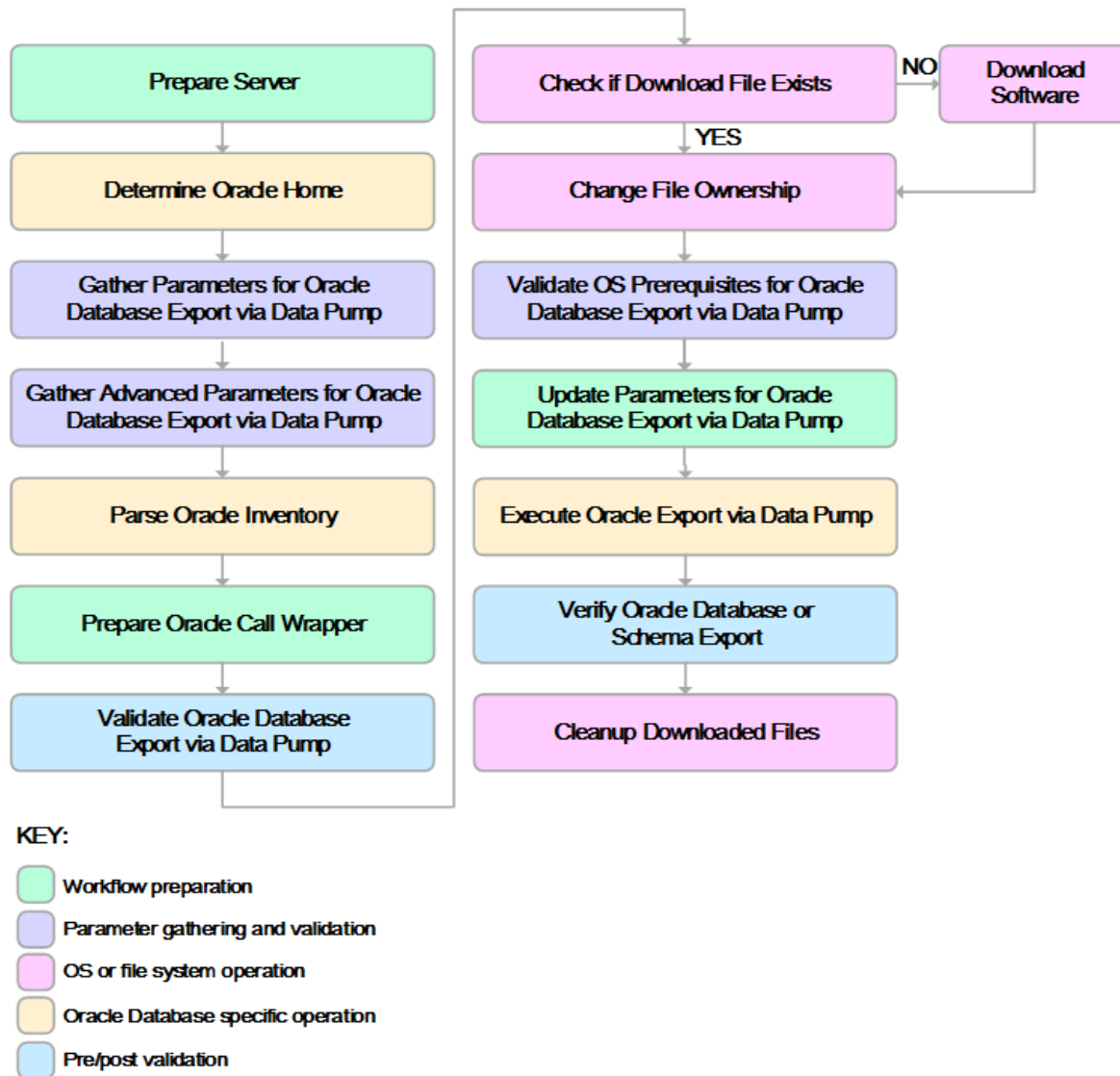
Validation Checks Performed

The workflow validates the following conditions:

1. The Oracle DB User user can connect to and query the database specified in the Oracle SID.
2. Oracle Database version 10.2 (or later) is installed at the specified (or automatically detected) Oracle Home.
3. For Oracle Database version 11.2 (or later), the Oracle DB User has DATAPUMP_EXP_FULL_DATABASE permission. For earlier supported versions, the Oracle DB User has EXP_FULL_DATABASE permission.
4. The operating system on the target server is a supported DMA platform.
5. A temporary directory required for file storage can be created on the target server.
6. Values specified for parameters are appropriate for the parameters.
7. The specified Ignorable Oracle Errors are, in fact, valid error codes.
8. The specified Data Pump Export File is a valid path and file name.
9. If a Data Pump Parameter file is specified, the file exists in the specified location.
10. If a Data Pump Parameter file is not specified, at least one schema is specified.
11. The specified Target Directory exists, either locally or on a network share, or it can be created.
12. The directory names included in the Do Not Remove list (if any) are valid.
13. The objects in Exclude are mutually exclusive of the objects in Include.
14. Flashback SCN and Flashback Time parameters are not used together. If Flashback Time is specified, it is in the proper time format.

Steps Executed

The "Oracle - Export Database via Data Pump" workflow includes the following steps. Each step must complete successfully before the next step can start. If a step fails, the workflow reports a failure, and all subsequent steps are skipped.



Process Flow

This workflow performs the following tasks:

1. Determines the target server platform type, and identifies the server call wrapper.
2. Determines the Oracle Home path and Oracle SID by reading the oratab file.
3. Gathers all required and optional parameters.
4. Determines the OS owner of the Oracle Home directory.
5. Prepares the instance call wrapper based on the specified Oracle User.
6. Validates all parameter values specified or derived.
7. Downloads the Data Pump Parameter File (if specified) from the software repository.
8. Creates a Data Pump parameter file (or updates the existing parameter file) using values specified on the Deployment page. If you do not specify a value for a particular parameter, the default value is used.
9. Performs the Data Pump Export operation. Optionally prints the export log file contents to console and history pages.
10. Verifies that the database is back online after the export:
 - No corrupted blocks exist.
 - No files are in backup mode.
 - Temporary table space is available.
11. Verifies that the Data Pump Export File exists in the Target Directory.
12. Removes any temporary files and directories used to perform the export.

How to Run this Workflow

The following instructions show you how to customize and run the ["Oracle - Export Database via Data Pump"](#) workflow in your environment.

The workflow provides default values for most parameters. These default values are usually sufficient for a "typical" export. You can override the defaults by specifying parameter values in the deployment. You can also expose additional parameters in the workflow, if necessary, to accomplish more advanced scenarios. Any parameters not explicitly specified in the deployment will have the default values listed in ["Parameters for Oracle - Export Database via Data Pump" on page 423](#)

Note: Before following this procedure, review the ["Prerequisites for this Workflow"](#), and ensure that all requirements are satisfied.

To use the Oracle - Export Database via Data Pump workflow:

1. Create a deployable copy of the workflow.
2. Determine the values that you will specify for the following parameters:

Parameter Name	Default Value	Required	Description
Data Pump Parameter File	no default	optional	Name of the Data Pump Export parameter file that you provide. If you do not specify the absolute path to the Parameter File, the workflow will look for the file in the Target Directory. If you do not specify a Parameter File, default Data Pump Export settings will be used for parameters not specified in the deployment.
Oracle Account	no default	optional	Oracle user that owns the ORACLE_HOME on the target Oracle database server. Required if an inventory file does not exist. Leave blank for Windows.
Target Directory	no default	required	Directory where the RMAN backup files will be placed. This directory must exist prior to workflow execution. The specified Oracle User must have READ and WRITE permissions for this directory. This directory must be accessible to the target database server.

Note: This is the minimum set of parameters required to run this workflow. You may specify values for the optional parameters in the gather advanced parameters set. You also may need to expose additional parameters depending on your objectives.

See ["Parameters for Oracle - Export Database via Data Pump" on page 423](#) for detailed descriptions of all input parameters for this workflow, including default values.

3. In the workflow editor, expose any additional parameters that you need. You will specify values for those parameters when you create the deployment or at runtime.

4. Save the changes to the workflow (click **Save** in the lower right corner).
5. Create a new deployment.
6. On the Parameters tab, specify values (or set the type to Runtime Value) for the required parameters listed in step 2 and any additional parameters that you have exposed. You do not need to specify values for those parameters whose default values are appropriate for your environment.
7. On the Targets tab, specify one or more targets for this deployment.
8. Save the deployment (click **Save** in the lower right corner).
9. Run the workflow using this deployment, specifying any runtime parameters.

To verify the results:

The workflow will complete and report SUCCESS on the Console if it has run successfully. If an error occurs during workflow execution, the error is logged, and the workflow terminates in the FAILURE state.

Sample Scenarios

This topic shows you how to use various parameters to achieve the following database backup scenarios in your environment using the "Oracle - Export Database via Data Pump" workflow:

Scenario 1: Perform an Export Using Default Settings and Store Export File Locally

This is the simplest Data Pump export scenario. In this example, the export file is stored on the local file system. The parameters shown here are visible by default.

In this scenario, the Data Pump Parameter File is not specified. The workflow will create its own parameter file using default values. The Oracle Account parameter is also not specified; it will be obtained from the Oracle inventory file (typically oratab).

The Target Directory will hold the Data Pump Export file (or files), which can subsequently be used to perform a database refresh on another target.

Parameter Name	Example Value	Description
Target Directory	/var/DPEExport/Full/May2012	Directory where the Data Pump dump and Parameter files will be staged on the target database server. This directory must be known to the Oracle instance.

Be sure that the default values for all remaining parameters are appropriate for your environment (see Parameters for Oracle - Export Database via Data Pump).

Scenario 2: Perform an Export Using Default Settings and Store Export File on a Network Share

This scenario is identical to Scenario 1, except that the Data Pump Export file will be stored on a network share. This eliminates the need to move files from one server to another. Data Pump Export files that are placed in a shared network directory can readily be used as an input to the Refresh Oracle Database via Data Pump workflow.

Parameter Name	Example Value	Description
Target Directory	myfileservr.mycompany.com: /uo1/nfs_share	Directory where the Data Pump dump and Parameter files will be staged on the target database server. This directory must be known to the Oracle instance.

Be sure that the default values for all remaining parameters are appropriate for your environment (see Parameters for Oracle - Export Database via Data Pump).

Scenario 3: Perform an Export Using Non-Default Parameters

The Export Oracle Database via Data Pump workflow provides many parameters that can be modified to suit your needs. For example, the Data Pump Export file generated by the workflow can be compressed, encrypted, or divided into standard-sized pieces. You can also tell the workflow to ignore specific Oracle errors that might arise during the export but would have no bearing on its outcome.

In this example, the Data Pump Export file is stored on the local file system. The first three parameters listed are visible by default; the remaining parameters must be exposed in the workflow so that they are available in the deployment.

Parameter Name	Example Value	Description
Data Pump Parameter File	<code>/var/DPEExport/Parms/myDPparameters.par</code>	Name of the Data Pump Export parameter file that is updated (or created) by this step. If you do not specify a Parameter File, default Data Pump Export settings will be used for parameters not specified in the deployment.
Oracle Account	oracle	Oracle user that owns the ORACLE_HOME on the target Oracle database server where the Data Pump export will be performed. Required if inventory does not exist. Leave blank for windows.
Target Directory	<code>/var/DPEExport/Output/Full/May2012</code>	Directory where the Data Pump dump and Parameter files will be staged on the target database server. This directory must be known to the Oracle instance.
Compression	DATA_ONLY	Items that will be compressed in the Data Pump Export dump file set. Valid settings are ALL, NONE, DATA_ONLY, METADATA_ONLY. <ul style="list-style-type: none"> DATA_ONLY: Compress only the table row data (must also specify DATA_ONLY or ALL for the Content parameter). METADATA_ONLY: Compress only the database object definitions (must also specify METADATA_ONLY or ALL for the Content parameter). ALL: Compress both the table row data and the database object definitions in the dump file set (must also specify ALL for the Content parameter). NONE: Nothing is compressed in the dump file set. <p>You must specify the same Compression setting for the export and any subsequent import operations.</p> <p>DATA_ONLY and ALL compression settings are only supported in Oracle Database Enterprise Edition. You must enable the Oracle Advanced Compression option to use these settings.</p>
Content	DATA_ONLY	What to include in the Data Pump Export dump file set. Valid settings are ALL, DATA_ONLY, or METADATA_

Parameter Name	Example Value	Description
		<p>ONLY.</p> <ul style="list-style-type: none"> • DATA_ONLY: Include only table row data. Do not include database object definitions. • METADATA_ONLY: Include only database object definitions. Do not include table row data. If you specify METADATA_ONLY, any index or table statistics later imported from the dump file set will be locked after the import. • ALL: Include both table row data and database object definitions in the dump file set. <p>You must specify the same Content setting for the export and any subsequent import operations.</p>
Encryption Mode	PASSWORD	<p>This setting determines how the dump file set will be encrypted and how it can later be decrypted during a subsequent Data Pump Import operation. Valid values are PASSWORD, TRANSPARENT, and DUAL.</p> <ul style="list-style-type: none"> • PASSWORD: Data Pump Export uses the Encryption Password to encrypt the dump file set. You must specify the same Encryption Password to perform a subsequent import. • TRANSPARENT: The Oracle encryption wallet is used to encrypt the dump file set using the Secure Sockets Layer (SSL) protocol. The encryption wallet must also be used to decrypt the dump file set during a subsequent import. You cannot specify an Encryption Password if you specify TRANSPARENT mode. • DUAL: During a subsequent import operation, the dump file set can either be decrypted transparently using the Oracle encryption wallet, or it can be decrypted by using the same Encryption Password that was used for the export. <p>DUAL and TRANSPARENT mode are only supported in Oracle Database Enterprise Edition.</p> <p>Note: To use DUAL or TRANSPARENT mode, you must enable Oracle Advanced Security.</p> <p>If Encryption Mode is specified, Encryption Password must also be specified.</p> <p>If no value is specified, the default workflow behavior is that there will be no encryption.</p>
Encryption Password	myencpwd	<p>Key used to ensure that any encrypted column data, metadata, or table data is re-encrypted before it is written to the dump file set. If you do not specify an Encryption Password—or specify TRANSPARENT for</p>

Parameter Name	Example Value	Description
	<p>Tip: To avoid having to re-enter passwords whenever they change, you can create a policy to provide them to the workflow.</p>	<p>the Encryption Mode—data will be written to the dump files in clear text form.</p> <p>Note the following:</p> <ul style="list-style-type: none"> • If you specify an Encryption Password for the export, and the Encryption Mode is PASSWORD, you must specify the same Encryption Password for any subsequent import operations. • The Encryption Password is required when Encryption Mode is PASSWORD or DUAL. • The Encryption Password is not valid when Encryption Mode is TRANSPARENT. • If you specify an Encryption Password but do not specify the Encryption Mode, the mode defaults to PASSWORD. <p>This parameter is only supported in Oracle Database Enterprise Edition.</p>
File Size	16GB	<p>Maximum size (in MByte) of each dump file in the dump file set. If any file in the dump file set reaches this size, that file is closed, and Data Pump attempts to create a new file.</p> <p>Specify an integer and one of the following units: B (bytes), KB (kilobytes), MB (megabytes), GB (gigabytes), or TB (terabytes). The default unit is bytes.</p> <p>The minimum valid file size is 4 kilobytes; the maximum valid file size is 16 terabytes.</p> <p>The actual size of a dump file may be slightly smaller depending on the size of the internal blocks used.</p>
Ignorable Oracle Errors	ORA-39083, ORA-00959, ORA-01917, ORA-01918, ORA-01435	Comma delimited list of Oracle errors to ignore while executing the Data Pump Export.
Oracle DB User	siteadmin	<p>Database user account (if other than sysdba) that will be used to perform the Data Pump Export.</p> <p>Note: For Oracle Database 11g R2 (and later), this user must have the DATAPUMP_EXP_FULL_DATABASE role, or the workflow will fail. For earlier versions, the user must have the EXP_FULL_DATABASE role.</p>
Oracle DB User Password	siteadminpwd	Password for the Oracle DB User. This is required when this user is not sysdba.

Parameter Name	Example Value	Description
	Tip: To avoid having to re-enter passwords whenever they change, you can create a policy to provide them to the workflow.	
Temporary File Location	/var/temp/ DP_temp_files	The location where all temporary output files will be placed. This directory will be removed at the completion of the workflow.

Be sure that the default values for all remaining parameters are appropriate for your environment (see Parameters for Oracle - Export Database via Data Pump).

Parameters for Oracle - Export Database via Data Pump

The following tables describe the required and optional input parameters for this workflow. Some of these parameters may not be initially visible in a deployment. For some parameters, if you do not specify a value for a parameter, a default value is assigned.

Parameters whose values are derived in one step and consumed by another step are not shown here.

Parameters Defined in this Step: Gather Parameters for Oracle Database Export via Data Pump

Parameter Name	Default Value	Required	Description
Data Pump Export File Name	see description	optional	Name (absolute path) of the Data Pump Export dump file (or files) that will be created from an existing Oracle database. The default is: Target Directory\Oracle SID.dmp
Data Pump Parameter File	no default	optional	Name of the Data Pump Export parameter file that you provide. If you do not specify the absolute path to the Parameter File, the workflow will look for the file in the Target Directory. If you do not specify a Parameter File, default Data Pump Export settings will be used for parameters not specified in the deployment.
Inventory Files	see description	optional	Comma separated list of Oracle inventory file names (with absolute paths). If not specified, set to the appropriate default value for the target server operating system. Defaults are: Solaris: /var/opt/oracle/oraInst.loc Linux: /etc/oraInst.loc Windows: %ProgramFiles%\Oracle\Inventory
Oracle Account	no default	optional	Oracle user that owns the ORACLE_HOME on the target Oracle database server. Required if an inventory file does not exist. Leave blank for Windows.
Oracle Home	no default	optional	The ORACLE_HOME to use if more than one home is found in the inventory file (or files).
Oracle SID	no default	required	The Oracle System ID (SID) of the target database.
Server Wrapper	jython	required	Command that will be used to construct the call wrapper. The workflow uses the call wrapper to execute subsequent steps as either the OS administrative user or the Oracle user who owns the pertinent ORACLE_HOME. For example: sudo su - root /opt/hp/dma/client/bin/jython.sh sudo su - sysdba /opt/hp/dma/client/bin/jython.sh
Target Directory	no default	required	Directory where the Data Pump Export dump file set and the Parameter file will be staged on the target database server. This directory must be known to the Oracle instance.

Parameters Defined in this Step: Gather Advanced Parameters for Oracle Database Export via Data Pump

Parameter Name	Default Value	Required	Description
Compression	ALL	optional	<p>Items that will be compressed in the Data Pump Export dump file set. Valid settings are ALL, NONE, DATA_ONLY, METADATA_ONLY.</p> <ul style="list-style-type: none"> DATA_ONLY: Compress only the table row data (must also specify DATA_ONLY or ALL for the Content parameter). METADATA_ONLY: Compress only the database object definitions (must also specify METADATA_ONLY or ALL for the Content parameter). ALL: Compress both the table row data and the database object definitions in the dump file set (must also specify ALL for the Content parameter). NONE: Nothing is compressed in the dump file set. <p>You must specify the same Compression setting for the export and any subsequent import operations.</p> <p>DATA_ONLY and ALL compression settings are only supported in Oracle Database Enterprise Edition. You must enable the Oracle Advanced Compression option to use these settings.</p>
Content	ALL	optional	<p>What to include in the Data Pump Export dump file set. Valid settings are ALL, DATA_ONLY, or METADATA_ONLY.</p> <ul style="list-style-type: none"> DATA_ONLY: Include only table row data. Do not include database object definitions. METADATA_ONLY: Include only database object definitions. Do not include table row data. If you specify METADATA_ONLY, any index or table statistics later imported from the dump file set will be locked after the import. ALL: Include both table row data and database object definitions in the dump file set. <p>You must specify the same Content setting for the export and any subsequent import operations.</p>
Encryption Mode	see description	optional	<p>This setting determines how the dump file set will be encrypted and how it can later be decrypted during a subsequent Data Pump Import operation. Valid values are PASSWORD, TRANSPARENT, and DUAL.</p> <ul style="list-style-type: none"> PASSWORD: Data Pump Export uses the Encryption Password to encrypt the dump file set. You must specify the same Encryption Password to perform a subsequent import. TRANSPARENT: The Oracle encryption wallet is used to encrypt the dump file set using the Secure Sockets

Parameters Defined in this Step: Gather Advanced Parameters for Oracle Database Export via Data Pump, continued

Parameter Name	Default Value	Required	Description
			<p>Layer (SSL) protocol. The encryption wallet must also be used to decrypt the dump file set during a subsequent import. You cannot specify an Encryption Password if you specify TRANSPARENT mode.</p> <ul style="list-style-type: none"> DUAL: During a subsequent import operation, the dump file set can either be decrypted transparently using the Oracle encryption wallet, or it can be decrypted by using the same Encryption Password that was used for the export. <p>DUAL and TRANSPARENT mode are only supported in Oracle Database Enterprise Edition.</p> <p>Note: To use DUAL or TRANSPARENT mode, you must enable Oracle Advanced Security.</p> <p>If Encryption Mode is specified, Encryption Password must also be specified.</p> <p>If no value is specified, the default workflow behavior is that there will be no encryption.</p>
Encryption Password	no default	optional	Encryption password. Only required when Encryption Mode is set.
Exclude	no default	optional	<p>Filter for the metadata—objects and object types—that you want to EXCLUDE from the export.</p> <p>For example: SCHEMA:="HR"</p>
File Size	200MB	optional	<p>Maximum size (in MByte) of each dump file in the dump file set. If any file in the dump file set reaches this size, that file is closed, and Data Pump attempts to create a new file.</p> <p>Specify an integer and one of the following units: B (bytes), KB (kilobytes), MB (megabytes), GB (gigabytes), or TB (terabytes). The default unit is bytes.</p> <p>The minimum valid file size is 4 kilobytes; the maximum valid file size is 16 terabytes.</p> <p>The actual size of a dump file may be slightly smaller depending on the size of the internal blocks used.</p>
Flashback SCN	no default	optional	SCN (System Change Number) used to reset the session snapshot.
Flashback Time	no default	optional	Time used to find the closest corresponding SCN (System Change Number) value. Format: DD-MM-YYYY HH24:MI:SS
Full	Y	optional	This parameter is set to Y to perform a full Data Pump Export (data and metadata) or N to only export schemas (metadata).
Ignorable	no default	optional	Comma delimited list of Oracle errors to ignore while

Parameters Defined in this Step: Gather Advanced Parameters for Oracle Database Export via Data Pump, continued

Parameter Name	Default Value	Required	Description
Oracle Errors			executing the Data Pump Export.
Include	no default	optional	Filter for the metadata—objects and object types for the current export mode—that you want to INCLUDE in the export. The specified objects and all their dependent objects are exported. Grants on these objects are also exported. For example: SCHEMA:="'HR'"
Job Name	no default	optional	Name of export job to be created.
Metrics	Y	optional	If you specify Y, the number of objects exported and the elapsed time required for the export operation to complete are recorded in the Data Pump log file. Valid values are Y or N.
Oracle DB User	sysdba	optional	Database user account (if other than sysdba) that will be used to perform the Data Pump Export. Note: For Oracle Database 11g R2 (and later), this user must have the DATAPUMP_EXP_FULL_DATABASE role, or the workflow will fail. For earlier versions, the user must have the EXP_FULL_DATABASE role.
Oracle DB User Password	/ as sysdba	optional	Password for the Oracle DB User. This is required when this user is not sysdba.
Parallel	1	optional	Number of active workers for current export job. If no value is specified, the default workflow behavior is 1.
Reuse	N	optional	If set to Y, the workflow overwrites the destination dump file (if it exists). Default behavior is N.
Schema	no default	optional	Comma separated list of schemas to export. Required if Data Pump Parameter File is not specified.
Show Log File	False	optional	If set to True, the workflow prints the export log file contents to console and history pages. Default value is False.
Statistics	no default	optional	A parameter comparable to STATISTICS is not needed. Statistics are always saved for tables.

Oracle - Refresh Database via Data Pump

This workflow imports a full Oracle database from a previously created Data Pump Export file (or files). The files can be located in the local file system or on a network share. You can use this workflow to implement a cross-platform database refresh (for example: Linux to Solaris).

Data Pump uses SQL commands to import and export specific data objects. It is slower than the Oracle Recovery Manager (RMAN) but offers more flexibility.

The workflow automatically detects which ORACLE_HOME and ORACLE_SID to use when performing the Data Pump import. You must specify the same encryption mode and password, compression level, and file size that was used for the export.

You have the option of providing a Data Pump parameter file or entering the parameters on the Deployment page. In either case, the parameter values are validated prior to the Data Pump import. If you do not provide a parameter file, the workflow creates one based on the parameter values that you specify on the Deployment page. If you do not specify a value for a particular parameter, the default value is used (see ["Parameters for Oracle - Refresh Database via Data Pump" on page 439](#)).

To use this workflow in your environment, see the following information:

Topic	Information Included
"Prerequisites for this Workflow"	List of prerequisites that must be satisfied before you can run this workflow
"How this Workflow Works"	Information about what the workflow does, including validation checks performed, steps executed, and a high-level process flow
"How to Run this Workflow"	Instructions for running this workflow in your environment
"Sample Scenarios"	Examples of typical parameter values for this workflow
"Parameters for Oracle - Refresh Database via Data Pump"	List of input parameters for this workflow

Note: The documentation for this workflow refers to the workflow and its steps by their base names. The names in the DMA user interface may have a version appended, for example, v2.

Note: To view the steps included in this workflow, see the [Steps for Oracle - Refresh Database via Data Pump](#).

Prerequisites for this Workflow

Be sure that the following prerequisites are satisfied before you run the ["Oracle - Refresh Database via Data Pump"](#) workflow:

1. The DMA client must be installed on all target servers.
2. The Target Directory must exist prior to the execution of the workflow. This directory can be local, or it can be a Network File System (NFS) mount point.

Note: If you specify an NFS mount point, the pertinent NFS share must be available to the target server, and it must be mounted prior to running this workflow.

3. The specified Oracle Database user must have READ and WRITE permission for the specified Target Directory.
4. The Oracle Database software must be provisioned, and the database must exist in the target instance prior to workflow execution.

Note: For Data Pump workflows, you must specify the same Content and Encryption Password settings for the export and any subsequent import operations.

For more information about prerequisites for Oracle Database, refer to the [Oracle Database Product Documentation](#).

How this Workflow Works

This topic contains the following information about the ["Oracle - Refresh Database via Data Pump"](#) workflow:

Overview

This workflow imports a full Oracle database from a previously created Data Pump Export file (or files). The files can be located in the local file system or on a network share. You can use this workflow to implement a cross-platform database refresh (for example: Linux to Solaris).

Data Pump uses SQL commands to import and export specific data objects. It is slower than the Oracle Recovery Manager (RMAN) but offers more flexibility.

The workflow automatically detects which ORACLE_HOME and ORACLE_SID to use when performing the Data Pump import. You must specify the same encryption mode and password, compression level, and file size that was used for the export.

You have the option of providing a Data Pump parameter file or entering the parameters on the Deployment page. In either case, the parameter values are validated prior to the Data Pump import. If you do not provide a parameter file, the workflow creates one based on the parameter values that you specify on the Deployment page. If you do not specify a value for a particular parameter, the default value is used (see ["Parameters for Oracle - Refresh Database via Data Pump" on page 439](#)).

You can use this workflow as part of a database refresh process. Database refresh involves moving the contents of a database in one Oracle instance into a database in another Oracle instance. This is useful, for example, if you want to move a database from a traditional IT infrastructure to a private cloud. It is also useful if you want to duplicate production data in a test environment for application development or troubleshooting purposes.

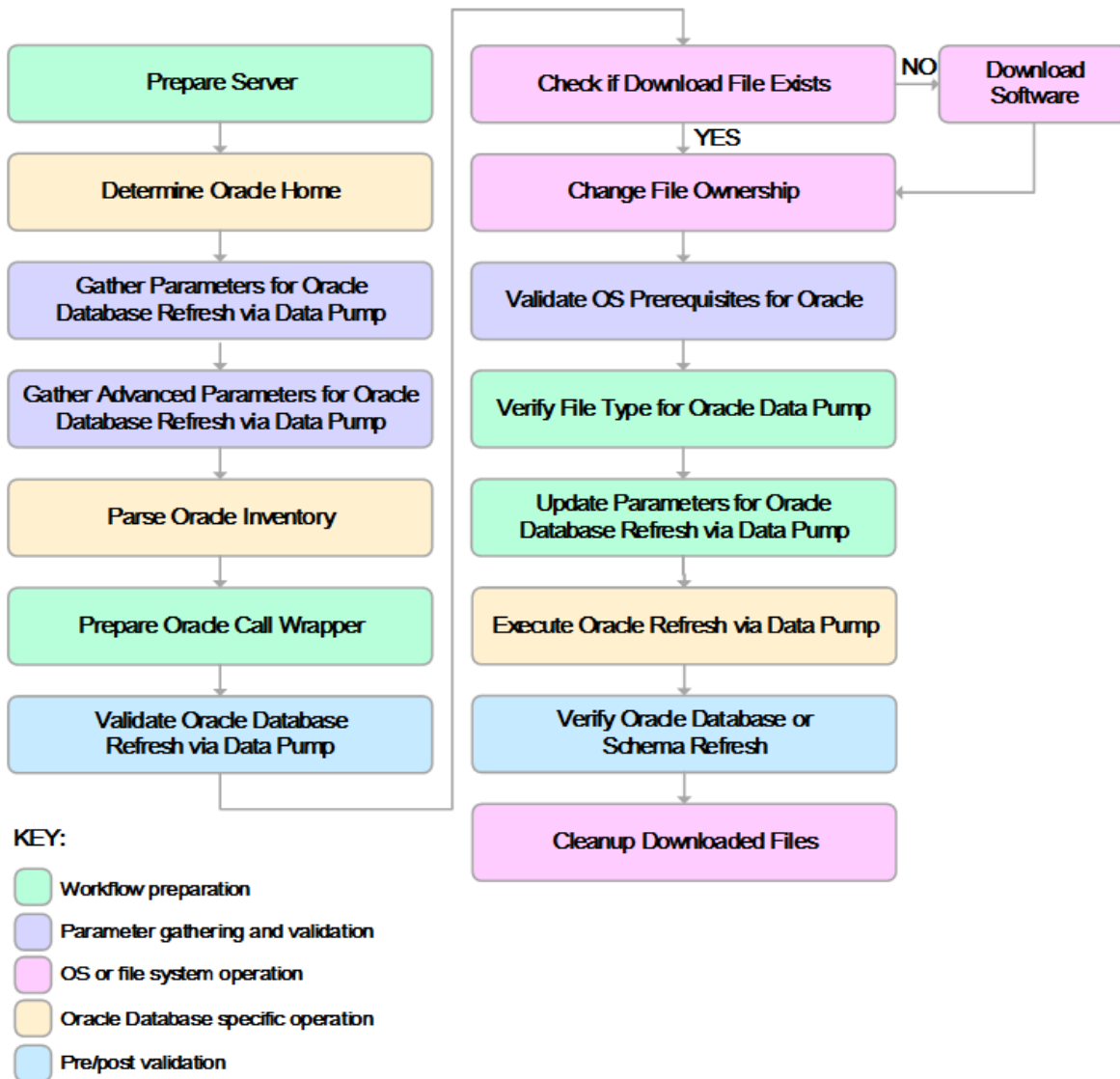
Validation Checks Performed

The workflow validates the following conditions:

1. The specified Oracle DB User can connect to and query the database specified in the Oracle SID.
2. Oracle Database version 10.2 (or later) is installed at the specified (or automatically detected) Oracle Home.
3. The Oracle DB User has permission to perform a full database export using the Data Pump utility. The Oracle Database user must have EXP_FULL_DATABASE permission.
4. A temporary directory required for file storage can be created on the target server.
5. The specified Ignorable Oracle Errors are, in fact, valid error codes.
6. The specified Data Pump Export File is a valid path and file name.
7. If a Data Pump Parameter file is specified, the file exists in the specified location.
8. The specified Target Directory exists, either locally or on a network share, and is writable.
9. The directory names included in the Do Not Remove list (if any) are valid.
10. The operating system on the target server is a supported DMA platform.
11. The specified Data Pump Export File was, indeed, created by Data Pump.

Steps Executed

The "Oracle - Refresh Database via Data Pump" workflow includes the following steps. Each step must complete successfully before the next step can start. If a step fails, the workflow reports a failure, and all subsequent steps are skipped.



Process Flow

This workflow performs the following tasks:

1. Determines the target server platform type, and identifies the server call wrapper.
2. Determines the Oracle Home path and Oracle SID by reading the oratab file.
3. Gathers all required and optional parameters.
4. Determines the OS owner of the Oracle Home directory.
5. Prepares the instance call wrapper based on the specified Oracle User.
6. Validates all parameter values specified or derived.
7. Downloads the Data Pump Parameter File, SQL Verification Script, and SQL Verification Results (if specified) from the software repository.
8. Creates a Data Pump parameter file (or updates the existing parameter file) using values specified on the Deployment page. If you do not specify a value for a particular parameter, the default value is used.
9. Performs the Data Pump Import operation.
10. Checks the Import Log File to ensure that it does not contain any unexpected errors.
11. Verifies that the database is online after the import:
 - No corrupted blocks exist.
 - No files are in backup mode.
 - Temporary table space is available.
12. Runs the SQL Verification Script (if provided), and compares the results to the SQL Verification Results (must be provided if the script is provided).
13. Removes any temporary files and directories used to perform the import.

How to Run this Workflow

The following instructions show you how to customize and run the ["Oracle - Refresh Database via Data Pump"](#) workflow in your environment.

The workflow provides default values for most parameters. These default values are usually sufficient for a "typical" export. You can override the defaults by specifying parameter values in the deployment. You can also expose additional parameters in the workflow, if necessary, to accomplish more advanced scenarios. Any parameters not explicitly specified in the deployment will have the default values listed in ["Parameters for Oracle - Refresh Database via Data Pump" on page 439](#)

Note: Before following this procedure, review the ["Prerequisites for this Workflow"](#), and ensure that all requirements are satisfied.

To use the Oracle - Refresh Database via Data Pump workflow:

1. Create a deployable copy of the workflow.
2. Determine the values that you will specify for the following parameters:

Parameter Name	Default Value	Required	Description
Data Pump Export Files	no default	required	Comma-separated list of Data Pump Export dump files included in the dump file set that will be used for this Data Pump Import. If only one file is specified, no comma is required.
Data Pump Parameter File	no default	optional	Name of the Data Pump Export parameter file that you provide. If you do not specify the absolute path to the Parameter File, the workflow will look for the file in the Target Directory. If you do not specify a Parameter File, default Data Pump Export settings will be used for parameters not specified in the deployment.
Oracle Account	no default	optional	Oracle user that owns the ORACLE_HOME on the target Oracle database server. Required if an inventory file does not exist. Leave blank for Windows.
Target Directory	no default	required	Directory where the RMAN backup files will be placed. This directory must exist prior to workflow execution. The specified Oracle User must have READ and WRITE permissions for this directory. This directory must be accessible to the target database server.

Note: This is the minimum set of parameters required to run this workflow. You may specify values for the optional parameters in the gather advanced parameters set. You also may need to expose additional parameters depending on your objectives.

See ["Parameters for Oracle - Refresh Database via Data Pump" on page 439](#) for detailed descriptions of all input parameters for this workflow, including default values.

3. In the workflow editor, expose any additional parameters that you need. You will specify values for those parameters when you create the deployment or at runtime.
4. Save the changes to the workflow (click **Save** in the lower right corner).
5. Create a new deployment.
6. On the Parameters tab, specify values (or set the type to Runtime Value) for the required parameters listed in step 2 and any additional parameters that you have exposed. You do not need to specify values for those parameters whose default values are appropriate for your environment.
7. On the Targets tab, specify one or more targets for this deployment.
8. Save the deployment (click **Save** in the lower right corner).
9. Run the workflow using this deployment, specifying any runtime parameters.

To verify the results:

The workflow will complete and report SUCCESS on the Console if it has run successfully. If an error occurs during workflow execution, the error is logged, and the workflow terminates in the FAILURE state.

Sample Scenarios

This topic shows you how to use various parameters to achieve the following database backup scenarios in your environment using the ["Oracle - Refresh Database via Data Pump"](#) workflow:

Scenario 1: Perform a Schema Import Using Default Settings and a Network Share Target Directory

This is the simplest Data Pump import scenario. In this example, the export file has been stored on a network share. The parameters shown here are visible by default.

In this scenario, the Data Pump Parameter File is not specified. The workflow will create its own parameter file using default values.

Parameter Name	Example Value	Description
Data Pump Export Files	april302012export.dmp	Comma-separated list of Data Pump Export dump files included in the dump file set that will be used for this Data Pump Import. If only one file is specified, no comma is required.
Oracle Account	sysdba	Oracle user that owns the ORACLE_HOME on the target Oracle database server where the Data Pump import will be performed. Required if inventory does not exist. Leave blank for windows.
Target Directory	myfileservr.mycompany.com:/uo1/nfs_share	Directory where the Data Pump dump and Parameter files will be staged on the target database server. This directory must be known to the Oracle instance.
Schema	hr,sh,oe	Comma separated list of schemas to be imported.

Be sure that the default values for all remaining parameters are appropriate for your environment.

Scenario 2: Perform a Schema Import Using a Parameter File that is Stored in the Software Repository

In this scenario, a Data Pump parameter file is used to specify all the Data Pump Import options—including the schemas that will be imported. In this case, the Data Pump Export file is located on a network share.

Parameter Name	Example Value	Description
Data Pump Export Files	april302012export.dmp	Comma-separated list of Data Pump Export dump files included in the dump file set that will be used for this Data Pump Import. If only one file is specified, no comma is required.
Data Pump Parameter File	myDPparameters.par	Name of the Data Pump Import parameter file that you provide. If you do not specify the absolute path to the Parameter File, the workflow will look for the file in the Target Directory. If you do not specify a Parameter File, default Data Pump Import settings will be used for parameters not specified in the deployment.
Oracle Account	sysdba	Oracle user that owns the ORACLE_HOME on the target Oracle database server where the Data Pump import will be performed. Required if inventory does not exist. Leave blank for windows.
Target Directory	myfileservers.mycompany.com: /uo1/nfs_share	Directory where the Data Pump dump and Parameter files will be staged on the target database server. This directory must be known to the Oracle instance.

Be sure that the default values for all remaining parameters are appropriate for your environment.

Scenario 3: Perform a Schema Import Using Non-Default Parameters

The "Oracle - Refresh Database via Data Pump" workflow provides many parameters that can be modified to suit your needs. You can instruct Data Pump how to proceed if it finds existing data in the database. You can also tell the workflow to ignore specific Oracle errors that might arise during the import but would have no bearing on its outcome.

In this example, the Data Pump Export file is stored on a network share. The first three parameters listed are visible by default; the remaining parameters must be exposed in the workflow so that they are available in the deployment.

Parameter Name	Example Value	Description
Data Pump Export Files	april302012export.dmp	Comma-separated list of Data Pump Export dump files included in the dump file set that will be used for this Data Pump Import. If only one file is specified, no comma is required.
Oracle Account	sysdba	Oracle user that owns the ORACLE_HOME on the target Oracle database server where the Data Pump import will be performed. Required if inventory does not exist. Leave blank for windows.
Target Directory	myfileservers.mycompany.com:/u01/nfs_share	Directory where the Data Pump dump and Parameter files will be staged on the target database server. This directory must be known to the Oracle instance.
Cleanup Database	True	If set to True, the workflow will clean up the database and will attempt to drop all non-default schemas. Default behavior is False.
Content	DATA_ONLY	What is included in the Data Pump Export dump file set. Valid settings are ALL, DATA_ONLY, or METADATA_ONLY. <ul style="list-style-type: none"> DATA_ONLY: Only table row data is included. Database object definitions are not included. METADATA_ONLY: Only database object definitions are included. Table row data is not included. If you specify METADATA_ONLY, any index or table statistics later imported from the dump file set will be locked after the import. ALL: Both table row data and database object definitions are included in the dump file set. You must specify the same Content setting for the export and any subsequent import operations.
Encryption Password	myencpwd	Encryption password. Only required when Encryption Mode was used during the export.

Parameter Name	Example Value	Description
Ignorable Oracle Errors	ORA-39111, ORA-39151, ORA-31685	Comma delimited list of Oracle errors to ignore while executing the Data Pump Import.
Oracle DB User	siteadmin	Database user account (if other than sysdba) that will be used to perform the Data Pump Import. Note: For Oracle Database 11g R2 (and later), this user must have the DATAPUMP_IMP_FULL_DATABASE role, or the workflow will fail. For earlier versions, the user must have the IMP_FULL_DATABASE role.
Oracle DB User Password	siteadminpwd	Required only if the DB User Password is not '/' as sysdba'.
Table Exist Action	REPLACE	This parameter tells the Data Pump Import utility what to do if a table that it is attempting to import already exists in the database. Valid values are: <ul style="list-style-type: none"> • SKIP leaves the table unchanged (no rows are imported from the dump file). • APPEND adds the rows from the dump file and leaves the existing rows unchanged. • TRUNCATE deletes the existing rows from the table and adds the rows from the dump file. • REPLACE removes the existing table and recreates it from the dump file. Note: SKIP and REPLACE are not valid options if Content is DATA_ONLY.
Temporary File Location	/var/temp/ DP_temp_files	Location to store temporary files while the workflow is running.

Be sure that the default values for all remaining parameters are appropriate for your environment.

Parameters for Oracle - Refresh Database via Data Pump

The following tables describe the required and optional input parameters for this workflow. Some of these parameters may not be initially visible in a deployment. For some parameters, if you do not specify a value for a parameter, a default value is assigned.

Parameters whose values are derived in one step and consumed by another step are not shown here.

Parameters Defined in this Step: Gather Parameters for Oracle Database Refresh via Data Pump

Parameter Name	Default Value	Required	Description
Data Pump Export Files	no default	required	Comma-separated list of Data Pump Export dump files included in the dump file set that will be used for this Data Pump Import. If only one file is specified, no comma is required.
Data Pump Parameter File	no default	optional	<p>Name of the Data Pump Import parameter file that you provide. You can also provide parameter that are not listed in the Gather Parameters for Oracle Database Refresh via Data Pump step or Gather Advanced Parameters for Oracle Database Refresh via Data Pump step. If you do not specify the absolute path to the Parameter File, the workflow will look for the file in the Target Directory. If you do not specify a Parameter File, default Data Pump Import settings will be used for parameters not specified in the deployment.</p> <p>The parameter values specified in the Data Pump Parameter File overwrites the default values.</p>
Inventory Files	see description	optional	<p>Comma separated list of Oracle inventory file names (with absolute paths). If not specified, set to the appropriate default value for the target server operating system. Defaults are:</p> <p>Solaris: /var/opt/oracle/oraInst.loc</p> <p>Linux: /etc/oraInst.loc</p> <p>Windows: %ProgramFiles%\Oracle\Inventory</p>
Oracle Account	no default	optional	Oracle user that owns the ORACLE_HOME on the target Oracle database server. Required if an inventory file does not exist. Leave blank for Windows.
Oracle Home	no default	optional	The ORACLE_HOME to use if more than one home is found in the inventory file (or files).
Oracle SID	no default	required	The Oracle System ID (SID) of the target database.
Server Wrapper	jython	required	<p>Command that will be used to construct the call wrapper. The workflow uses the call wrapper to execute subsequent steps as either the OS administrative user or the Oracle user who owns the pertinent ORACLE_HOME. For example:</p> <pre>sudo su - root /opt/hp/dma/client/bin/jython.sh sudo su - sysdba /opt/hp/dma/client/bin/jython.sh</pre>

Parameters Defined in this Step: Gather Parameters for Oracle Database Refresh via Data Pump, continued

Parameter Name	Default Value	Required	Description
Target Directory	no default	required	Directory where the Data Pump Export dump file set and the Parameter file will be staged on the target database server. This directory must be known to the Oracle instance.

Parameters Defined in this Step: Gather Advanced Parameters for Oracle Database Refresh via Data Pump

Parameter Name	Default Value	Required	Description
Cleanup Database	False	optional	If set to True, the workflow will clean up the database and will attempt to drop all non-default schemas. Default behavior is False.
Cleanup Users Exclude	no default	optional	Comma separated list of database users that should be excluded from the cleanup process.
Content	ALL	optional	<p>What is included in the Data Pump dump file set that will be imported. Valid settings are ALL, DATA_ONLY, or METADATA_ONLY.</p> <ul style="list-style-type: none"> • DATA_ONLY: Include only table row data. Do not include database object definitions. • METADATA_ONLY: Include only database object definitions. Do not include table row data. If you specify METADATA_ONLY, any index or table statistics later imported from the dump file set will be locked after the import. • ALL: Include both table row data and database object definitions in the dump file set. <p>You must specify the same Content setting for the export and any subsequent import operations.</p>
Data Options	no default	optional	Options for how to handle certain types of data during exports and imports. The only valid option for this parameter is SKIP_CONSTRAINT_ERRORS.
Encryption Password	no default	optional	Encryption password. Only required when Encryption Mode was used during the export.
Exclude	no default	optional	<p>Filter for the metadata—objects and object types—that you want to EXCLUDE from the import.</p> <p>For example: SCHEMA:="'HR'"</p>
Ignorable Oracle Errors	ORA-31684, ORA-39111, ORA-39151, ORA-31685,	optional	Comma delimited list of Oracle errors to ignore while executing the Data Pump Import.

Parameters Defined in this Step: Gather Advanced Parameters for Oracle Database Refresh via Data Pump, continued

Parameter Name	Default Value	Required	Description
	ORA-00001		
Include	no default	optional	Filter for the metadata—objects and object types for the current import mode—that you want to INCLUDE in the import. For example: SCHEMA:="'HR'"
Job Name	no default	optional	Name of the import job to be created.
Oracle DB User	sysdba	optional	Database user account (if other than sysdba) that will be used to perform the Data Pump Import. Note: For Oracle Database 11g R2 (and later), this user must have the DATAPUMP_IMP_FULL_DATABASE role, or the workflow will fail. For earlier versions, the user must have the IMP_FULL_DATABASE role.
Oracle DB User Password	/ as sysdba	optional	Password for the Oracle DB User. This is required when this user is not sysdba.
Parallel	1	optional	Number of active workers for current import job. If no value is specified, the default workflow behavior is 1.
Partition Options	no default	optional	This parameter specifies how table partitions will be created by providing a value for PARTITION_OPTIONS in the Data Pump Import operation. Valid values are: <ul style="list-style-type: none"> NONE creates tables as they existed on the system from which the export operation was performed. DEPARTITION promotes each partition or subpartition to a new individual table. MERGE combines all partitions and subpartitions into one table.
Remap Data	no default	optional	This parameter allows you to remap data by providing a value for REMAP_TABLE in the Data Pump Import operation. For example: TABLE_NAME1.COLUMN1:TABLE_NAME2.COLUMN2
Remap Datafile	no default	optional	Comma separated list of key value pairs separated by a colon. Changes the name of the source datafile to the target datafile name in all SQL statements where the source datafile is referenced: CREATE TABLESPACE, CREATE LIBRARY, and CREATE DIRECTORY. Example Format: '/u01/app/oracle/oradata/orca/scott1.dbf': '/u01/app/oracle/oradata/orcb/scott1.dbf', '/u01/app/oracle/oradata/orca/scott2.dbf':

Parameters Defined in this Step: Gather Advanced Parameters for Oracle Database Refresh via Data Pump, continued

Parameter Name	Default Value	Required	Description
			'/u01/app/oracle/oradata/orcb/scott2.dbf')
Remap Tablespace	no default	optional	<p>This parameter allows you to remap all objects selected for import with persistent data in the source tablespace to be created in the target tablespace by providing a value for REMAP_TABLESPACE in the Data Pump Import operation.</p> <p>For example: TABLE_SPACE1:TABLE_SPACE2</p>
Schema	no default	optional	Comma separated list of schemas to be imported.
Show Log File	False	optional	If set to True, the workflow prints the import log file contents to console and history pages. Default value is False.
Table Exist Action	SKIP	optional	<p>This parameter tells the Data Pump Import utility what to do if a table that it is attempting to import already exists in the database. Valid values are:</p> <ul style="list-style-type: none"> • SKIP leaves the table unchanged (no rows are imported from the dump file). • APPEND adds the rows from the dump file and leaves the existing rows unchanged. • TRUNCATE deletes the existing rows from the table and adds the rows from the dump file. • REPLACE removes the existing table and recreates it from the dump file. <p>Note: SKIP and REPLACE are not valid options if Content is DATA_ONLY.</p>
Tables	no default	optional	Comma separated list of tables to be imported.
Tablespaces	no default	optional	Comma separated list of tablespaces to be imported.
Update System Tables	False	optional	<p>Determines whether the system tables are updated during the Data Pump Import. If TRUE, all system tables will be included in the import. If FALSE, the SYS and SYSMGR tables are excluded from the import. This is useful, because importing these tables often generates numerous errors, each of which must otherwise be added to the Ignorable Oracle Errors list.</p> <p>You can explicitly specify a list of tables to be excluded from the import by using the Schema parameter in the Update Parameters for Oracle Database Refresh via Data Pump step.</p>
Verification Result	no default	optional	<p>Name (with absolute path) of a text file containing the expected results of the SQL queries included in the Verification SQL Script.</p> <p>This parameter is required if you provide a Verification</p>

Parameters Defined in this Step: Gather Advanced Parameters for Oracle Database Refresh via Data Pump, continued

Parameter Name	Default Value	Required	Description
			<p>SQL Script. Be sure to run the Verification SQL Script on the SOURCE database before running this workflow, and copy the results into this file.</p> <p>You must provide this file in a location where the workflow can access it.</p>
Verification SQL Script	no default	optional	<p>Name (with absolute path) of a text file containing a SQL script that verifies the integrity of the database.</p> <p>You must provide this file in a location where the workflow can access it. The expected results of the queries included in this script must be provided in the Verification Result file.</p>
XML Password	xdb	optional	<p>XML password. If the XDB schema is present and cleanup is set to True then the XML database will be re-created. Oracle requires the XML database password to be provided in the event that the XML database is re-created.</p>

Oracle - Migrate Database TTS

This workflow migrates a database from a known source database to a known destination database by using a shared staging directory that is available to both the source and the destination. The staging directory can be a Network File System (NFS) mount. You can use this workflow to implement a cross-platform migration (for example: Linux to Solaris).

If the operating systems on the two targets warrant, the workflow also converts the `endian` format during the migration. (Endianness is either big-endian or little-endian and does not depend directly on Oracle software because it is a platform (hardware+OS) property that is used by Oracle software.) If endian conversion is necessary, the workflow uses Transportable Tablespace (TTS) cross-platform migration with both Data Pump and RMAN; you choose whether to convert on the source side or the destination side. If `endian` conversion is not necessary, then the workflow uses Data Pump in a standard TTS method.

If the destination has a higher Oracle version, the workflow also upgrades the Oracle version.

This workflow is especially useful in the following cases:

- For refreshing very large databases
- When you plan to move your database from older hardware to newer hardware

You specify the parameters on the Deployment page. The parameter values are validated prior to the migration. If you do not specify a value for a particular parameter, the default value is used (see ["Parameters for Oracle - Migrate Database TTS"](#)).

Note: This workflow is a **bridged execution** workflow. You specify PRIMARY TARGET and DESTINATION at run-time.

To use this workflow in your environment, see the following information:

Topic	Information Included
"Prerequisites for this Workflow"	List of prerequisites that must be satisfied before you can run this workflow
"How this Workflow Works"	Information about what the workflow does, including validation checks performed, steps executed, and a high-level process flow
"How to Run this Workflow"	Instructions for running this workflow in your environment
"Sample Scenarios"	Examples of typical parameter values for this workflow
"Parameters for Oracle - Migrate Database TTS"	List of input parameters for this workflow

Note: To view the workflow steps, see [Steps for Oracle - Migrate Database TTS](#).

Prerequisites for this Workflow

Be sure that the following prerequisites are satisfied before you run the ["Oracle - Migrate Database TTS"](#) workflow:

1. The Primary Target (source) and Destination must both be available as targets within DMA. In other words, you must run the Discovery workflow beforehand to "discover" them as targets.
2. A single, temporary target directory (staging directory) must exist and be available to both the Primary Target and the Destination prior to the execution of the workflow. This directory can be local, or it can be a Network File System (NFS) mount point. The directory is the Source Target Directory on the Primary Target and is the Destination Target Directory on the Destination.

Note: If you specify an NFS mount point, the pertinent NFS share must be available to the target servers and mounted prior to running this workflow. These are example NFS mount commands for Linux and Solaris:

Linux	<pre>mount -t nfs -o rw,rsize=32768, wsize=32768,tcp,hard,nointr, nfsvers=3,bg,actimeo=0,timeo=600, suid,async <ServerName>: /u01/nfs_share /u01/nfs_share</pre>	<p><ServerName> is the server name where the NFS mount point is created</p> <p>/u01/nfs_share is an example of the NFS mount shared directory</p>
Solaris	<pre>share -F nfs -o rw,anon=0 -d "<InstallServerDirectory>" /var/tmp/nfs_share</pre>	<p><InstallServerDirectory> is the directory name where the NFS mount point is created</p> <p>/var/tmp/nfs_share is an example of the NFS mount shared directory</p>

3. The Oracle user account that owns the Oracle binaries must have read and write privileges on both Source Target Directory and Destination Target Directory.
4. The Oracle Database software must be provisioned, and the database must exist in the Primary Target prior to workflow execution.
5. The DMA client must be installed on all target servers.
6. The Oracle version on the destination must be the same or higher than the Oracle version on the source.
7. The same character set must be used on both the Primary Target and the Destination.
8. The Tablespaces must be self-contained. You must move both the Tablespace and the users at the same time.

For more information about prerequisites for Oracle Database, refer to the [Oracle Database Product Documentation](#).

How this Workflow Works

This topic contains the following information about the ["Oracle - Migrate Database TTS"](#) workflow:

Overview

This workflow performs a database migration and/or upgrade from a known source database to a destination database. The destination database must already be provisioned and discovered using Oracle's Transportable Tablespace (TTS) method.

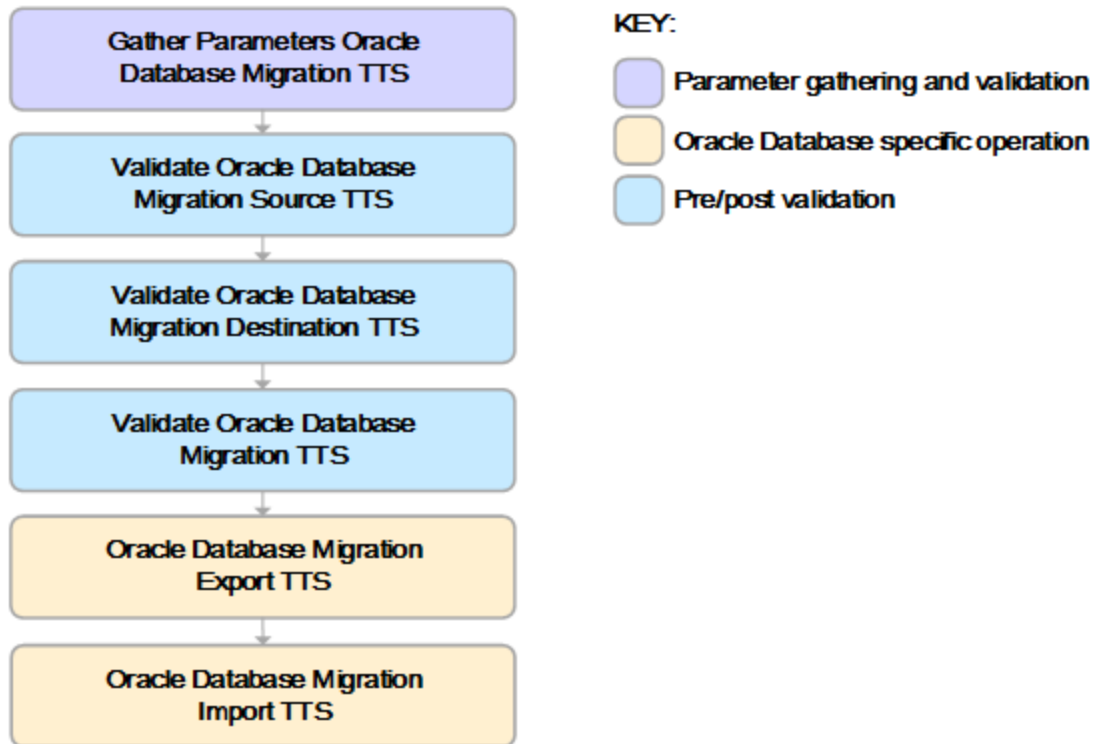
The workflow determines the operating systems where the databases reside. If endian conversion is necessary, then the workflow uses TTS cross-platform migration (both Data Pump and RMAN). If endian conversion is not necessary, then Data Pump is used in a standard Transportable Tablespace refresh method.

You enter the parameters on the Deployment page. The parameter values are validated prior to the migration. If you do not specify a value for a particular parameter, the default value is used (see ["Parameters for Oracle - Migrate Database TTS"](#)).

Note: This workflow is a **bridged execution** workflow. You specify the SOURCE and DESTINATION targets at run-time.

Steps Executed

The "Oracle - Migrate Database TTS" workflow includes the following steps. Each step must complete successfully before the next step can start. If a step fails, the workflow reports a failure, and all subsequent steps are skipped.



Process Flow

This workflow performs the following tasks on the SOURCE target server (Primary Target):

1. Gathers all required and optional parameters.
2. Validates the following:
 - The values of the parameters entered on the deployment page and assigns default values if not specified.
 - The Conversion Host is source or destination.
 - The Oracle Account owns Oracle Home.
 - The Oracle Home exists.
 - The target directory exists and is writable.
 - Oracle Errors have the correct format.
 - The database is ready for TTS migration.
 - The archive log mode.
 - Oracle Enterprise Edition.
3. Prepares the target directory and changes the permissions, if necessary.
4. Determines OS type and endian values.

The workflow then performs the following tasks on the DESTINATION target server:

5. Validates the following:
 - Oracle Account owns Oracle Home.
 - The Oracle Home exists.
 - The target directory exists and is writable.
 - The database is ready for TTS migration.
 - Oracle Enterprise Edition.
6. Prepares the target directory and changes the permissions, if necessary.
7. Determines OS type and endian values.

The workflow then performs the following tasks on the SOURCE target server (Primary Target):

8. Determines the migration option based on the OSes and endians.
9. Validates the following:
 - The Oracle version on the destination is the same (or higher) than the source.
 - Disk Parallelism is a number.
 - The charactersets are compatible.

10. If Pre-Check Only is True, the workflow ends.
11. Creates the target directory.
12. Performs a Data Pump export of the migration metadata.
13. Assigns full user grants for export database.
14. If conversion is necessary and is to be done on SOURCE, then runs an RMAN endian conversion, or else simply copies the data files.

The workflow then performs the following tasks on the DESTINATION target server:

15. Creates the target directory.
16. Assigns full user grants on the import database.
17. If conversion is necessary and is to be done on DESTINATION, then runs an RMAN endian conversion in place, or else simply copies the data files.
18. Performs a Data Pump import of the migration metadata.

How to Run this Workflow

The following instructions show you how to customize and run the ["Oracle - Migrate Database TTS"](#) workflow in your environment.

The workflow provides default values for most parameters. These default values are usually sufficient for a "typical" export. You can override the defaults by specifying parameter values in the deployment. You can also expose additional parameters in the workflow, if necessary, to accomplish more advanced scenarios. Any parameters not explicitly specified in the deployment will have the default values listed in ["Parameters for Oracle - Migrate Database TTS"](#).

Note: Before following this procedure, review the ["Prerequisites for this Workflow"](#), and ensure that all requirements are satisfied, particularly that the staging directory is available and mounted.

To use the Oracle - Migrate Database TTS workflow:

1. Create a deployable copy of the workflow.
2. Determine the values that you will specify for the following parameters:

Parameter Name	Default Value	Required	Description
Conversion Host	Destination	optional	If endian conversions are necessary, the host where the conversions take place. Valid values: Source or Destination.
Destination	no default	required	Name of the destination database (migrated to).
Destination Target Directory	no default	required	Staging directory path known to the DESTINATION Database Server and shared with the SOURCE Database Server. For example, the path to the NFS mount point as known by the DESTINATION Database Server.
Source Target Directory	no default	required	Staging directory path known to the SOURCE Database Server and shared with the DESTINATION Database Server. For example, the path to NFS mount point as known by SOURCE Database Server. For Solaris NFS, these mount options are recommended: mount -o rw,bg,intr,hard,timeo=600, wsize=32768,rsize=32768

Note: This is the minimum set of parameters required to run this workflow. You may need to expose additional parameters depending on your objectives.

See ["Parameters for Oracle - Migrate Database TTS"](#) for detailed descriptions of all input parameters for this workflow, including default values.

3. In the workflow editor, expose any additional parameters that you need. You will specify values for these parameters when you create the deployment.
4. Save the changes to the workflow (click **Save** in the lower right corner).
5. Create a new deployment.
 - a. On the Targets tab, select all the target servers—both source and destination—that will participate in this database migration. The targets that you select here will be available in the Target Parameters drop-down menus on the Run page (see [step 7](#)).
 - b. On the Parameters tab, specify values for the required parameters listed in [step 2](#) and any additional parameters that you exposed in [step 3](#). You do not need to specify values for those parameters whose default values are appropriate for your environment.
6. Save the deployment (click **Save** in the lower right corner).
7. Run the workflow using this deployment.

On the Run page, select the following targets from the respective drop-down menus:

Parameter Name	Default	Description
Primary Target	no default	Instance that contains the database that will be exported.
Destination	no default	Instance where the database will be imported.

To verify the results:

The workflow will complete and report SUCCESS on the Console if it has run successfully. If an error occurs during workflow execution, the error is logged, and the workflow terminates in the FAILURE state.

Sample Scenarios

This topic shows you how to use various parameters to achieve the following database backup scenarios in your environment using the ["Oracle - Migrate Database TTS"](#) workflow:

Scenario 1: Perform a Database Migration between two Solaris systems

This is the simplest Data Pump database migration scenario. In this example, the export file is stored on a network share to minimize data transfer overhead. The parameters shown here are visible by default.

In this scenario, the Data Pump Parameter File is not specified for either the export or the import. The workflow will create its own parameter files using default values. The Oracle Account parameter is also not specified; it will be obtained from the Oracle inventory file (typically `oratab`) on the SOURCE and DESTINATION target servers, respectively.

Parameter Name	Example Value	Description
Conversion Host		If endian conversions are necessary, the host where the conversions take place. Valid values: Source or Destination.
Destination		Name of the destination database (migrated to).
Destination Target Directory	<code>/var/tmp/nfs_destination</code>	Staging directory path known to the DESTINATION Database Server and shared with the SOURCE Database Server. For example, the path to the NFS mount point as known by the DESTINATION Database Server.
Source Target Directory	<code>/var/tmp/nfs_source</code>	<p>Staging directory path known to the SOURCE Database Server and shared with the DESTINATION Database Server. For example, the path to NFS mount point as known by SOURCE Database Server.</p> <p>For Solaris NFS, these mount options are recommended:</p> <pre>mount -o rw,bg,intr,hard,timeo=600, wsiz=32768,rsiz=32768</pre>

Be sure that the default values for all remaining parameters are appropriate for your environment (see ["Parameters for Oracle - Migrate Database TTS"](#)).

Scenario 2: Perform a Database Migration pre-check between two Solaris systems

This is almost the same as the previous Data Pump database migration scenario except this time you will only do a pre-check without performing the actual migration. This will validate that the source and destination databases are compatible and are ready for a migration. You need to expose the Pre-Check Only parameter in the workflow so that it is available in the deployment.

Parameter Name	Example Value	Description
Conversion Host		If endian conversions are necessary, the host where the conversions take place. Valid values: Source or Destination.
Destination		Name of the destination database (migrated to).
Destination Target Directory	/var/tmp/nfs_destination	Staging directory path known to the DESTINATION Database Server and shared with the SOURCE Database Server. For example, the path to the NFS mount point as known by the DESTINATION Database Server.
Pre-Check Only	True	If set to True, then only the pre-check steps will run.
Source Target Directory	/var/tmp/nfs_source	<p>Staging directory path known to the SOURCE Database Server and shared with the DESTINATION Database Server. For example, the path to NFS mount point as known by SOURCE Database Server.</p> <p>For Solaris NFS, these mount options are recommended:</p> <pre>mount -o rw,bg,intr,hard,timeo=600, wsize=32768,rsize=32768</pre>

Be sure that the default values for all remaining parameters are appropriate for your environment (see ["Parameters for Oracle - Migrate Database TTS"](#)).

Parameters for Oracle - Migrate Database TTS

The following tables describe the required and optional input parameters for this workflow. Some of these parameters may not be initially visible in a deployment. For some parameters, if you do not specify a value for a parameter, a default value is assigned.

Parameters Defined in this Step: Gather Parameters Oracle Database Migration TTS

Parameter Name	Default Value	Required	Description
Conversion Host	Destination	optional	If <code>endian</code> conversions are necessary, the host where the conversions take place. Valid values: Source or Destination.
Destination	no default	required	Name of the destination database (migrated to).
Destination Target Directory	no default	required	Staging directory path known to the DESTINATION Database Server and shared with the SOURCE Database Server. For example, the path to the NFS mount point as known by the DESTINATION Database Server.
Disk Parallelism	1	optional	RMAN Disk Parallelism to be set when disabling and re-enabling RMAN compression. Specifies how many channels (up to 254) RMAN should allocate for jobs on the specified device type.
Ignorable Oracle Errors	ORA-31684,ORA-39111,ORA-39151,ORA-31685,ORA-00001	optional	Comma-separated list of Oracle Errors to ignore if found during the migration process.
Oracle Account	no default	required	Operation system account that owns the Oracle Home installation.
Pre-Check Only	False	optional	If set to True, then only the pre-check steps will run.
Source Target Directory	no default	required	Staging directory path known to the SOURCE Database Server and shared with the DESTINATION Database Server. For example, the path to NFS mount point as known by SOURCE Database Server. For Solaris NFS, these mount options are recommended: <code>mount -o rw,bg,intr,hard,timeo=600,wsiz=32768,rsiz=32768</code>

Oracle - Drop Database

The Oracle Drop Database enables you to remove the target database from the Oracle instance and from the DMA environment.

To use this workflow in your environment, see the following information:

Topic	Information Included
"Prerequisites for this Workflow" on the next page	List of prerequisites that must be satisfied before you can run this workflow
"How this Workflow Works" on page 458	Information about what the workflow does, including validation checks performed, steps executed, and step descriptions
" How to Run this Workflow" on page 459	Instructions for running this workflow in your environment
"Parameters for Oracle - Drop Database" on page 461	List of input parameters for this workflow

Prerequisites for this Workflow

Be sure that the following prerequisites are satisfied before you run the Oracle Drop Database workflow:

- This solution requires DMA version 10.30 (or later).

The latest DMA solution packs require the latest DMA platform. To use the latest solution packs, update the DMA platform. DMA10.50.001.000 solution packs are supported on DMA10.50.001.000 (and later).

- You have installed the Database Compliance solution pack.

The workflow must be able to:

- Get the Oracle instance up and running.
- Log in to the Oracle instance using Oracle login credentials.
- Drop the database upon connecting to the Oracle instance.

The information presented here assumes the following:

- DMA is installed and operational.
- At least one suitable target server is available.
- You are logged in to the DMA web interface.
- You have permission to create, edit, and deploy copies of the workflows included in this solution pack.

For more information about prerequisites for Oracle database, refer to the [Oracle Server Documentation](#).

How this Workflow Works

This workflow performs the following actions:

Drops an Oracle database and removes it from the DMA environment.

Steps Executed by the Workflow

The ["Oracle - Drop Database" on page 456](#) workflow includes the following steps. Each step must complete successfully before the next step can start. If a step fails, the workflow reports a failure and all subsequent steps are skipped.

Steps Used by Oracle

Workflow Step	Description
Gather Parameters for Drop Oracle Database	This step gathers parameters prior to executing the rest of the workflow.
Drop Oracle Database	This steps drops the Oracle database from the target machine.
Remove Instance from Environment	This step removes the Oracle database from the DMA environment.

Note: For input parameter descriptions and defaults, see ["Parameters for Oracle - Drop Database" on page 461](#).

How to Run this Workflow

The following instructions show you how to customize and run the Oracle Drop Database workflow in your environment.

The workflow provides default values for some parameters. These default values are usually sufficient for a "typical" installation. You can override the defaults by specifying parameter values in the deployment. You can also expose additional parameters in the workflow, if necessary, to accomplish more advanced scenarios. Any parameters not explicitly specified in the deployment will have the default values listed in ["Parameters for Oracle - Drop Database" on page 461](#).

Note: Before following this procedure, review the ["Prerequisites for this Workflow" on page 457](#), and ensure that all requirements are satisfied.

To use the Run Oracle Drop Database workflow:

1. Create a deployable copy of the workflow.
2. Determine the values that you will specify for the parameters.

Note: There are no mandatory parameters required to run this workflow. All parameters are optional. You may need to expose additional parameters depending on your objectives.

See ["Parameters for Oracle - Drop Database" on page 461](#) for detailed descriptions of all input parameters for this workflow, including default values.

3. In the workflow editor, expose any additional parameters that you need. You will specify values for those parameters when you create the deployment or at runtime.
4. Save the changes to the workflow (click **Save** in the lower right corner).
5. Create a new deployment.
6. On the Parameters tab, specify values (or set the type to Runtime Value) for the required parameters listed in step 2 and any additional parameters that you have exposed. You do not need to specify values for those parameters whose default values are appropriate for your environment.
7. On the Targets tab, specify one or more targets for this deployment.
8. Save the deployment (click **Save** in the lower right corner).
9. Run the workflow using this deployment, specifying any runtime parameters.

To verify the results:

The workflow will complete and report SUCCESS on the Console if it has run successfully. If an error occurs during workflow execution, the error is logged, and the workflow terminates in the FAILURE state. The database will be removed from the DMA environment section upon SUCCESS as well.

Parameters for Oracle - Drop Database

There are no mandatory parameters required to run this workflow. All parameters are optional. Some of these parameters are not initially visible in a deployment. For most parameters, if you do not specify a value for a parameter, a default value is assigned.

Oracle - Provision Data Guard v6

This workflow enables you to provision the Standby database for an already provisioned standby host and ORACLE_HOME and then to set up Data Guard.

This workflow is designed to run in an Oracle 11.2 (or later) database environment in RAC or Non-RAC setups. It is currently supported on Oracle-supported Linux and AIX platforms.

To use this workflow in your environment, see the following information:

Topic	Information Included
"Prerequisites for this Workflow" on the next page	List of prerequisites that must be satisfied before you can run this workflow
"How this Workflow Works" on page 465	Information about what the workflow does, including validation checks performed, steps executed, and step descriptions
" How to Run this Workflow" on page 467	Instructions for running this workflow in your environment
"Parameters for Oracle - Provision Data Guard" on page 469	List of input parameters for this workflow

Tip: To patch Server Automation Grid standalone environments, see *Achieve Patch Related Compliance for Oracle Grid Standalone Environments Using DMA*.

To patch more complex Oracle clustered environments, see *Achieve Patch Related Compliance for Oracle RAC Environments Using DMA*.

These documents are available at: <https://softwaresupport.hpe.com/>.

Prerequisites for this Workflow

Before performing the procedures in this section, your environment must meet the following minimum requirements:

- DMA version 10.50.001.000 (or later) with the Advanced Database Provisioning Solution Pack installed
- Servers running one of the following operating systems:
 - Linux (any version that is supported by Oracle and DMA)
 - AIX
 - Solaris

- Oracle 11.2.0.x or 12.1.0.x with the following Oracle configuration:

The Oracle Grid Infrastructure is installed on both the primary cluster servers and the standby cluster servers.

The Oracle database software is installed on all cluster servers.

Your primary database and your primary cluster already exist.

Tip: The following DMA workflows can help you achieve this configuration:

DMAOracle - Provision or Upgrade Grid Infrastructure

DMAOracle - Provision Database Software

DMAOracle - Provision Database

- The primary node of the primary cluster is able to `ssh` as root to ALL nodes in the standby cluster.
- Licenses for Oracle Database and DMA.
- This workflow requires Oracle Database Enterprise Edition version 11.2 (or later). It assumes that the primary database is already provisioned and running and the standby host is available with an RDBMS ORACLE_HOME provisioned. These can be met with workflows Provision Oracle Home and Provision an Oracle Database.
- This workflow also requires root and oracle user ID equivalence across all primary and standby database servers represented in the Data Guard setup. This workflow will regenerate the RSA keys for the Oracle user, setup passwordless SSH login, and add the details of all nodes on all the nodes in `/etc/hosts` file.
- Root and oracle userid equivalence must exist between the nodes in the Primary RAC and the

nodes in the Standby RAC. The use of this workflow is only supported in an Oracle 11.2 environment.

Tip: If you are configuring data guard in an Oracle Grid standalone environment, the prerequisites are appropriately simplified. For detailed instructions to provision this environment, see *Standardize Oracle Grid Standalone Provisioning Using DMA*, available at <https://softwaresupport.hpe.com/>

For more information about prerequisites for Oracle database, refer to the [Oracle Server Documentation](#).

How this Workflow Works

This workflow performs the following actions:

Enables you to provision the Standby database for an already provisioned standby host and ORACLE_HOME and then to set up Data Guard.

Steps Executed by the Workflow

The Oracle - Provision Data Guard v5 workflow includes the following steps. Each step must complete successfully before the next step can start. If a step fails, the workflow reports a failure and all subsequent steps are skipped.

Steps Used by Oracle - Provision Data Guard v5

Workflow Step	Description
Gather Parameters for Provision Oracle Data Guard v3	This step gathers all required input parameters needed for the Provision Oracle Data Guard workflow.
Gather Advanced Parameters for Provision Oracle Data Guard	This step gathers all optional (advanced) parameters needed for the Data Guard Provisioning workflow.
Set Oracle Provision Data Guard Prerequisites v2	This step updates the /etc/hosts file on the primary and standby servers by adding the details of all the nodes on all the nodes and will establish password-less ssh communication between all the primary and standby servers for the Oracle user.
Prepare Oracle Instance	This step prepares instance level Oracle access. Dependencies: IMPORTANT: Be sure to run this step as a user with read access to all specified inventory pointers (Linux/UNIX) or inventory files (Windows).
Validate Provision Oracle Data Guard	This step validates all parameters for the Provision Oracle Data Guard workflow.
Gather Primary DB Attributes v3	This step gathers all required input parameters needed for the Provision Oracle Data Guard workflow.
Enable ArchiveLog Mode AndOr Force Logging v2	This step will enable archive logging and forced logging on the target database in order to configure Data Guard.
Set Data Guard Primary DB Initialization Parameters v2	This step will configure the initialization parameters for the target database to support Data Guard.
Setup Standby Redo Logs on Primary Database	This step creates the standby redo logs on the primary database needed for Data Guard to successfully synchronize databases.
Setup Network Configuration on Primary and Standby Servers v5	This step sets up your tnsnames.ora and listener.ora files required for Data Guard to communicate to and from primary and standby databases.

Steps Used by Oracle - Provision Data Guard v5, continued

Workflow Step	Description
Update oratab on Standby Server v2	This step adds oratab entries for the standby database to be created on the standby nodes.
Create Required Directories on Standby Servers v4	This step creates directories that will be required once the standby database is replicated to the standby nodes.
Setup Password File for Data Guard v2	This step creates the password file on the primary and standby databases using the same password as required by Data Guard.
Create temporary initialization file on Standby server	This step creates the temporary initialization parameter file for the standby database.
Startup Listener on Standby Servers	This step starts the standby listeners if not already online.
Startup Instance Nomount on First Standby Server v2	This step starts the standby database in nomount mode to allow RMAN at a later point to run duplicate database commands.
Run RMAN Duplicate with Standby Init Parameters v4	This step uses RMAN to duplicate a primary database to a standby database location that has already been prepared.
Check Standby Database Status	This step verifies that a standby database reports that its database role is set to STANDBY.
Relocate SPFILE for Standby Database	This step will move the spfile for the standby database to proper location.
Multiplex Control Files on Standby v2	This step will multiplex the control files if the user has specified multiple control file locations.
Cluster Enable Standby Database v2	This step will cluster enable your standby database so it can belong to a RAC environment.
Register Standby Database with CRS v2	This step configures the standby database with CRS(Grid) home so CRS can manage the RAC database.
Verify Standby Database is up-to-date with Primary	This step will log in to both the primary and standby databases and obtain the log file sequence and compare to ensure the standby database is current with the primary database.

Note: For input parameter descriptions and defaults, see ["Parameters for Oracle - Provision Data Guard" on page 469](#).

How to Run this Workflow

The following instructions show you how to customize and run the Oracle - Provision Data Guard workflow in your environment.

The workflow provides default values for some parameters. These default values are usually sufficient for a "typical" installation. You can override the defaults by specifying parameter values in the deployment. You can also expose additional parameters in the workflow, if necessary, to accomplish more advanced scenarios. Any parameters not explicitly specified in the deployment will have the default values listed in ["Parameters for Oracle - Provision Data Guard" on page 469](#).

Note: Before following this procedure, review the ["Prerequisites for this Workflow" on page 463](#), and ensure that all requirements are satisfied.

To use the Oracle - Provision Data Guard workflow:

1. Create a deployable copy of the workflow.
2. Determine the values that you will specify for the parameters.

Note: There are no mandatory parameters required to run this workflow. All parameters are optional. You may need to expose additional parameters depending on your objectives.

See ["Parameters for Oracle - Provision Data Guard" on page 469](#) for detailed descriptions of all input parameters for this workflow, including default values.

3. In the workflow editor, expose any additional parameters that you need. You will specify values for those parameters when you create the deployment or at runtime.
4. Save the changes to the workflow (click **Save** in the lower right corner).
5. Create a new deployment.
6. On the Parameters tab, specify values (or set the type to Runtime Value) for the required parameters listed in step 2 and any additional parameters that you have exposed. You do not need to specify values for those parameters whose default values are appropriate for your environment.
7. On the Targets tab, specify one or more targets for this deployment.
8. Save the deployment (click **Save** in the lower right corner).
9. Run the workflow using this deployment, specifying any runtime parameters.

To verify the results:

The workflow will complete and report SUCCESS on the Console if it has run successfully. If an error occurs during workflow execution, the error is logged, and the workflow terminates in the FAILURE state. The database will be removed from the DMA environment section upon SUCCESS as well.

Parameters for Oracle - Provision Data Guard

The following tables describe the required and optional input parameters for this workflow. Some of these parameters may not be initially visible in a deployment. For some parameters, if you do not specify a value for a parameter, a default value is assigned.

Input Parameters Defined in this Step: Gather Parameters for Provision Oracle Data Guard v3

Parameter Name	Example Value	Required	Description
Database Protection Mode	Maximum Availability	required	<p>Data Guard database protection mode. Valid values are:</p> <p>Maximum Performance Transactions commit after the redo data required to recover those transactions is written to the online redo log</p> <p>Maximum Availability Transactions commit after the redo data is written to the online redo log and the standby redo log on at least one synchronized standby database</p> <p>Maximum Protection Similar to Maximum Availability, except that the primary database shuts down if it cannot write its redo stream to at least one synchronized standby database</p>
Oracle OS Password	●●●	required	OS level password for Oracle Account. This password will be used to set password less ssh between primary and secondary nodes
Oracle OS User	oracle	required	Oracle OS username used to derive primary node database properties.
Oracle sys Password	●●●	required	SYS Password for the primary and secondary databases.
Primary Node Hostnames	dma-rac1.mycompany.com, dma-rac2.mycompany.com	required	<p>Comma-separated list of primary database server host names or IP addresses.</p> <p>If more than one IP address/hostname is entered, it indicates that the primary database is on RAC.</p>
Standby DB Prefix Name	DR	required	Prefix that is appended to the DB_NAME to become the DB_UNIQUE_NAME for the standby databases.
Standby Node Hostnames	dma-rac3.mycompany.com, dma-rac4.mycompany.com	required	<p>Comma-separated list of up to 30 standby database server host names or IP addresses.</p> <p>If more than one IP address/hostname is entered, it indicates that the standby database is on RAC.</p>

Input Parameters Defined in this Step: Gather Advanced Parameters for Provision Oracle Data Guard

Parameter Name	Example Value	Required	Description
Archive Lag Target	600	optional	Specifies the maximum time (in seconds) by which the standby database can lag behind the primary database. Valid values are 0 (zero) or 60-7200 seconds. If you specify Archive Lag Target, you must also specify Standby DB Unique Name.
Change Remote Login PasswordFile on Primary	?	optional	Set to Yes if DMA is permitted to change the value of the Remote_Login_Passwordfile init.ora parameter to EXCLUSIVE (if it is not already set to EXCLUSIVE on the primary database). The default is Yes.
DB File Name Convert	?	optional	Used only if the primary and standby database datafiles will reside in different locations on the respective servers. Specify an even number of strings: "string1","string2","string3","string4",... where string 1 is a sequence of characters in the primary database datafile name, string 2 is a sequence of characters in the first standby database datafile name, string 3 is a sequence of characters in the second primary database datafile name, string 4 is a sequence of characters in the second standby database datafile name, and so on. Each string must be delimited with single or double quotes. For example: "newyork","chicago","newyork","atlanta".
Data Guard Standby Type	Physical	optional	The type of standby databases that you are configuring. Valid values are Physical, Logical, or Snapshot (only Physical is currently implemented). The default is Physical.
Listener File Location	?	optional	Fully-qualified filename for the listener file. This is only needed for non-standard installs. Do not specify if using the default file \$ORACLE_HOME/network/admin/listener.ora or the listener runs from a non-ASM home while ASM is in use.
Location for Controlfiles on Standby Server	?	optional	Comma-separated list of fully-qualified controlfile filenames to create multiple copies of the controlfile on the standby database. By default, only one controlfile is generated on the standby database. The paths must already exist on the target servers.
Log Archive Dest 1	?	optional	The target destination for the archived logfiles on the primary database (if it is not already set in the primary database). The default is none.
Log File Name Convert	?	optional	Used only if the primary and standby redo log files will reside in different locations on the respective servers. Specify an even number of strings: "string1","string2","string3","string4",... where string 1 is a sequence of characters in the primary database redo log file name, string 2 is a sequence of characters in the first standby database redo log file name, string 3 is a sequence of characters in the second primary database redo log file name, string 4 is a sequence of characters in the second standby database redo log file

Input Parameters Defined in this Step: Gather Advanced Parameters for Provision Oracle Data Guard, continued

Parameter Name	Example Value	Required	Description
			name, and so on. Each string must be delimited with single or double quotes. For example: "newyork","chicago","newyork", "atlanta".
Number of RMAN Auxiliary Channels	?	optional	Number of RMAN (Recovery Manger) auxiliary channels to be used during the RMAN duplicate database process.
Number of RMAN Primary Channels	?	optional	Number of RMAN (Recovery Manger) primary channels to be used during the RMAN duplicate database process. The default is 2.
Oracle sys Password	?	optional	SYS Password for the primary and secondary databases. (Required to be mapped from the Gather Parameters step.) Will be used to default the value of Password File password parameter.
Oratab File Location	?	optional	Fully-qualified path to the oratab file. The default is /etc/oratab
Password File password	?	optional	The password to set in the password file orapw. The default is the Oracle sys Password.
Primary DB Listener Port Number	?	optional	Port number for the primary database listener. The default is the Oracle default.
Standby DB Listener Port Number	?	optional	Port number for the standby database listener. The default is the Oracle default.
Tnsnames File Location	?	optional	Fully-qualified filename for the TNS (Transparent Network Substrate) file. This is only needed for non-standard installs. Do not specify if using the default file \$ORACLE_HOME/network/admin/tnsnames.ora
Update oratab file on Standby Servers	?	optional	Set to Yes to update the oratab file on standby servers. The default is Yes.

Oracle - Create Data Guard Broker Configuration

This workflow enables you to deploy a Data Guard Broker configuration on Oracle 11.2 (or later) databases with Data Guard successfully installed and set up.

This workflow is designed to run in an Oracle 11.2 (or later) database environment where Oracle Data Guard has been provisioned. It is currently supported on Oracle-supported Linux and AIX platforms.

To use this workflow in your environment, see the following information:

Topic	Information Included
"Prerequisites for this Workflow" on the next page	List of prerequisites that must be satisfied before you can run this workflow
"How this Workflow Works" on page 475	Information about what the workflow does, including validation checks performed, steps executed, and step descriptions
"How to Run this Workflow" on page 476	Instructions for running this workflow in your environment
"Parameters for Oracle - Create Data Guard Broker Configuration" on page 478	List of input parameters for this workflow

Tip: To patch Server Automation Grid standalone environments, see *Achieve Patch Related Compliance for Oracle Grid Standalone Environments Using DMA*.

To patch more complex Oracle clustered environments, see *Achieve Patch Related Compliance for Oracle RAC Environments Using DMA*.

These documents are available at: <https://softwaresupport.hpe.com/>.

Prerequisites for this Workflow

Before performing the procedures in this section, your environment must meet the following minimum requirements:

- DMA version 10.50.001.000 (or later) with the Advanced Database Provisioning Solution Pack installed
- Servers running one of the following operating systems:
 - Linux (any version that is supported by Oracle and DMA)
 - AIX
 - Solaris

- Oracle 11.2.0.x or 12.1.0.x with the following Oracle configuration:

The Oracle Grid Infrastructure is installed on both the primary cluster servers and the standby cluster servers.

The Oracle database software is installed on all cluster servers.

Your primary database and your primary cluster already exist.

Tip: The following DMA workflows can help you achieve this configuration:

DMAOracle - Provision or Upgrade Grid Infrastructure

DMAOracle - Provision Database Software

DMAOracle - Provision Database

- The primary node of the primary cluster is able to `ssh` as root to ALL nodes in the standby cluster.
- Licenses for Oracle Database and DMA.
- This workflow requires Oracle Database Enterprise Edition version 11.2 (or later). It assumes that the primary database is already provisioned and running and the standby host is available with an RDBMS ORACLE_HOME provisioned. These can be met with workflows Provision Oracle Home and Provision an Oracle Database.
- This workflow also requires root and oracle user ID equivalence across all primary and standby database servers represented in the Data Guard setup. This workflow will regenerate the RSA keys for the Oracle user, setup passwordless SSH login, and add the details of all nodes on all the nodes in `/etc/hosts` file.

Tip: If you are configuring data guard in an Oracle Grid standalone environment, the prerequisites are appropriately simplified. For detailed instructions to provision this environment, see

Standardize Oracle Grid Standalone Provisioning Using DMA, available at
<https://softwaresupport.hpe.com/>

For more information about prerequisites for Oracle database, refer to the [Oracle Server Documentation](#).

How this Workflow Works

This workflow performs the following actions:

Enables you to deploy a Data Guard Broker configuration on Oracle 11.2 (or later) databases with Data Guard successfully installed and set up.

Steps Executed by the Workflow

The Oracle - Create Data Guard Broker Configuration workflow includes the following steps. Each step must complete successfully before the next step can start. If a step fails, the workflow reports a failure and all subsequent steps are skipped.

Steps Used by Oracle - Create Data Guard Broker Configuration

Workflow Step	Description
Gather Parameters for Create Data Guard Broker Configuration	This step gathers all required input parameters needed for this workflow.
Validate Create Data Guard Broker Configuration	This step validates the input parameters required to create data guard blocker configuration.
Build Data Guard Broker Configuration v2	<p>This step creates a Data Guard Broker configuration by performing the following actions:</p> <ol style="list-style-type: none">1. Makes sure that the Data Guard Broker is installed on the primary database server and has not yet been configured.2. Gets the DB_UNIQUE_NAME for the primary and each standby database.3. Creates the Broker configuration.4. Checks the status of the Broker configuration.

Note: For input parameter descriptions and defaults, see ["Parameters for Oracle - Create Data Guard Broker Configuration" on page 478](#).

How to Run this Workflow

The following instructions show you how to customize and run the Oracle - Create Data Guard Broker Configuration workflow in your environment.

The workflow provides default values for some parameters. These default values are usually sufficient for a "typical" installation. You can override the defaults by specifying parameter values in the deployment. You can also expose additional parameters in the workflow, if necessary, to accomplish more advanced scenarios. Any parameters not explicitly specified in the deployment will have the default values listed in ["Parameters for Oracle - Create Data Guard Broker Configuration" on page 478](#).

Note: Before following this procedure, review the ["Prerequisites for this Workflow" on page 473](#), and ensure that all requirements are satisfied.

To use the Oracle - Create Data Guard Broker Configuration workflow:

1. Create a deployable copy of the workflow.
2. Determine the values that you will specify for the parameters.

Note: There are no mandatory parameters required to run this workflow. All parameters are optional. You may need to expose additional parameters depending on your objectives.

See ["Parameters for Oracle - Create Data Guard Broker Configuration" on page 478](#) for detailed descriptions of all input parameters for this workflow, including default values.

3. In the workflow editor, expose any additional parameters that you need. You will specify values for those parameters when you create the deployment or at runtime.
4. Save the changes to the workflow (click **Save** in the lower right corner).
5. Create a new deployment.
6. On the Parameters tab, specify values (or set the type to Runtime Value) for the required parameters listed in step 2 and any additional parameters that you have exposed. You do not need to specify values for those parameters whose default values are appropriate for your environment.
7. On the Targets tab, specify one or more targets for this deployment.
8. Save the deployment (click **Save** in the lower right corner).
9. Run the workflow using this deployment, specifying any runtime parameters.

To verify the results:

The workflow will complete and report SUCCESS on the Console if it has run successfully. If an error occurs during workflow execution, the error is logged, and the workflow terminates in the FAILURE state. The database will be removed from the DMA environment section upon SUCCESS as well.

Parameters for Oracle - Create Data Guard Broker Configuration

The following tables describe the required and optional input parameters for this workflow. Some of these parameters may not be initially visible in a deployment. For some parameters, if you do not specify a value for a parameter, a default value is assigned.

Input Parameters Defined in this Step: Gather Parameters for Create Data Guard Broker Configuration

Parameter Name	Example Value	Required	Description
Connect Identifier		required	The connect identifier used to connect to the primary database. It is defined in the <code>tnsnames.ora</code> file. Make sure that the <code>tnsnames.ora</code> file on every database and instance that is part of the configuration contains an entry for this connect identifier.
Data Guard Broker Config Name	broker12c	required	The name that will be assigned to the Broker configuration that you are creating.
Data Guard Standby Type	Physical	required	The type of standby databases that you are configuring. Valid values are Physical, Logical, or Snapshot (only Physical is currently implemented).
Oracle sys Password	●●●	required	SYS Password for the primary and secondary databases.
Oracle user name		required	Owner of the Oracle database software.
Primary Node Hostnames	dma-rac1.mycompany.com, dma-rac2.mycompany.com <i>Use the same value(s) as the Primary Node Hostnames parameter for the Oracle - Provision Data Guard v3 deployment.</i>	required	Comma-separated list of primary database server host names or IP addresses. If more than one IP address/hostname is entered, it indicates that the primary database is on RAC.
Standby Connect Identifier	DRorca <i>Use the value of the Standby DB Prefix Name parameter for the Oracle - Provision Data Guard v3 deployment plus the target's primary database name.</i>	required	Comma-separated list of the connect strings used to connect to the standby databases. These are defined in the <code>tnsnames.ora</code> file. Make sure that the <code>tnsnames.ora</code> file on every

Input Parameters Defined in this Step: Gather Parameters for Create Data Guard Broker Configuration, continued

Parameter Name	Example Value	Required	Description
			database and instance that is part of the configuration contains an entry for these connect identifiers.
Standby Node Hostnames	dma-rac3.mycompany.com, dma-rac4.mycompany.com <i>Use the same value(s) as the Standby Node Hostnames parameter for the Oracle - Provision Data Guard v3 deployment.</i>		Comma-separated list of up to 30 standby database server host names or IP addresses. If more than one IP address/hostname is entered, it indicates that the standby database is on RAC.

Oracle - Configure Data Guard Broker Properties

This workflow enables you to configure the Data Guard Broker Properties for existing Oracle 11.2 (or later) databases in a Data Guard configuration.

This workflow is designed to run in an Oracle 11.2 (or later) database environment where Oracle Data Guard has been provisioned. It is currently supported on Oracle-supported Linux and AIX platforms.

To use this workflow in your environment, see the following information:

Topic	Information Included
"Prerequisites for this Workflow" on the next page	List of prerequisites that must be satisfied before you can run this workflow
"How this Workflow Works" on page 483	Information about what the workflow does, including validation checks performed, steps executed, and step descriptions
"How to Run this Workflow" on page 484	Instructions for running this workflow in your environment
"Parameters for Oracle - Configure Data Guard Broker Properties" on page 486	List of input parameters for this workflow

Tip: To patch Server Automation Grid standalone environments, see *Achieve Patch Related Compliance for Oracle Grid Standalone Environments Using DMA*.

To patch more complex Oracle clustered environments, see *Achieve Patch Related Compliance for Oracle RAC Environments Using DMA*.

These documents are available at: <https://softwaresupport.hpe.com/>.

Prerequisites for this Workflow

Before performing the procedures in this section, your environment must meet the following minimum requirements:

- DMA version 10.50.001.000 (or later) with the Advanced Database Provisioning Solution Pack installed
- Servers running one of the following operating systems:
 - Linux (any version that is supported by Oracle and DMA)
 - AIX
 - Solaris

- Oracle 11.2.0.x or 12.1.0.x with the following Oracle configuration:

The Oracle Grid Infrastructure is installed on both the primary cluster servers and the standby cluster servers.

The Oracle database software is installed on all cluster servers.

Your primary database and your primary cluster already exist.

Tip: The following DMA workflows can help you achieve this configuration:

DMAOracle - Provision or Upgrade Grid Infrastructure

DMAOracle - Provision Database Software

DMAOracle - Provision Database

- The primary node of the primary cluster is able to `ssh` as `root` to ALL nodes in the standby cluster.
- Licenses for Oracle Database and DMA.
- This workflow requires Oracle Database Enterprise Edition version 11.2 (or later). It assumes that the primary database is already provisioned and running and the standby host is available with an RDBMS `ORACLE_HOME` provisioned. These can be met with workflows Provision Oracle Home and Provision an Oracle Database.
- This workflow also requires root and oracle user ID equivalence across all primary and standby database servers represented in the Data Guard setup. This workflow will regenerate the RSA keys for the Oracle user, setup passwordless SSH login, and add the details of all nodes on all the nodes in `/etc/hosts` file.

Tip: If you are configuring data guard in an Oracle Grid standalone environment, the prerequisites are appropriately simplified. For detailed instructions to provision this environment, see

Standardize Oracle Grid Standalone Provisioning Using DMA, available at
<https://softwaresupport.hpe.com/>

For more information about prerequisites for Oracle database, refer to the [Oracle Server Documentation](#).

How this Workflow Works

This workflow performs the following actions:

Enables you to configure the Data Guard Broker Properties for existing Oracle 11.2 (or later) databases in a Data Guard configuration.

Steps Executed by the Workflow

The Oracle - Configure Data Guard Broker Properties workflow includes the following steps. Each step must complete successfully before the next step can start. If a step fails, the workflow reports a failure and all subsequent steps are skipped.

Steps Used by Oracle - Configure Data Guard Broker Properties

Workflow Step	Description
Gather Parameters for Configure Data Guard Broker Properties	This step gathers all required input parameters needed for this workflow.
Validate Configure Data Guard Broker Properties	This step validates the input parameters required to configure data guard blocker properties.
Configure Data Guard Broker Properties	<p>This step enables you to modify the state and properties of a Data Guard Broker configuration or a specific database within it. You can use this step to perform any of the following:</p> <ul style="list-style-type: none"> • Change the LogXptMode parameter, which controls the redo data transport service (SYNC or ASYNC). • Start or stop the Redo Apply service on the specified standby database servers (APPLY-ON or APPLY-OFF). • Start or stop transmitting the redo data from the primary database server (TRANSPORT-ON or TRANSPORT-OFF). • Enable or disable Broker management of this configuration (ENABLE or DISABLE). • Disable Broker management of specific standby database. • Change the ArchiveLagTarget parameter, which determines how far the standby database lag the primary database (zero or 60-7200 seconds).

Note: For input parameter descriptions and defaults, see ["Parameters for Oracle - Configure Data Guard Broker Properties" on page 486](#).

How to Run this Workflow

The following instructions show you how to customize and run the Oracle - Configure Data Guard Broker Properties workflow in your environment.

The workflow provides default values for some parameters. These default values are usually sufficient for a "typical" installation. You can override the defaults by specifying parameter values in the deployment. You can also expose additional parameters in the workflow, if necessary, to accomplish more advanced scenarios. Any parameters not explicitly specified in the deployment will have the default values listed in ["Parameters for Oracle - Configure Data Guard Broker Properties" on page 486](#).

Note: Before following this procedure, review the ["Prerequisites for this Workflow" on page 481](#), and ensure that all requirements are satisfied.

To use the Oracle - Configure Data Guard Broker Properties:

1. Create a deployable copy of the workflow.
2. Determine the values that you will specify for the parameters.

Note: There are no mandatory parameters required to run this workflow. All parameters are optional. You may need to expose additional parameters depending on your objectives.

See ["Parameters for Oracle - Configure Data Guard Broker Properties" on page 486](#) for detailed descriptions of all input parameters for this workflow, including default values.

3. In the workflow editor, expose any additional parameters that you need. You will specify values for those parameters when you create the deployment or at runtime.
4. Save the changes to the workflow (click **Save** in the lower right corner).
5. Create a new deployment.
6. On the Parameters tab, specify values (or set the type to Runtime Value) for the required parameters listed in step 2 and any additional parameters that you have exposed. You do not need to specify values for those parameters whose default values are appropriate for your environment.
7. On the Targets tab, specify one or more targets for this deployment.
8. Save the deployment (click **Save** in the lower right corner).
9. Run the workflow using this deployment, specifying any runtime parameters.

To verify the results:

The workflow will complete and report SUCCESS on the Console if it has run successfully. If an error occurs during workflow execution, the error is logged, and the workflow terminates in the FAILURE state. The database will be removed from the DMA environment section upon SUCCESS as well.

Parameters for Oracle - Configure Data Guard Broker

Properties

The following tables describe the required and optional input parameters for this workflow. Some of these parameters may not be initially visible in a deployment. For some parameters, if you do not specify a value for a parameter, a default value is assigned.

Input Parameters Defined in this Step: Gather Parameters for Configure Data Guard Broker Properties

Parameter Name	Example Value	Required	Description
Archive Lag Target	600	optional	Specifies the maximum time (in seconds) by which the standby database can lag behind the primary database. Valid values are 0 (zero) or 60-7200 seconds. If you specify Archive Lag Target, you must also specify Standby DB Unique Name.
Broker Config State	ENABLE	optional	Enables or disables Broker management of the primary and all standby databases in the specified Broker configuration. Valid values are ENABLE or DISABLE.
Disable Standby DB		optional	Comma-separated list of up to 30 standby databases for which Broker management will be disabled. For Oracle - Configure Data Guard Broker Properties - not yet implemented.
LogXptMode	SYNC	optional	Sets the redo transport service on the specified standby databases. Valid Values are SYNC or ASYNC. SYNC ensures the highest level of data protection for the primary database, but it also incurs the highest performance impact. You must use SYNC for maximum protection and maximum availability modes. ASYNC offers a moderate grade of data protection for the primary database and incurs a lower performance impact than SYNC.

Input Parameters Defined in this Step: Gather Parameters for Configure Data Guard Broker Properties, continued

Parameter Name	Example Value	Required	Description
Oracle sys Password	●●●	required	SYS Password for the primary and secondary databases.
Oracle user name	Oracle	required	Owner of the Oracle database software.
Primary Node Hostnames	dma-rac1.mycompany.com, dma-rac2.mycompany.com <i>Use the same value(s) as the Primary Node Hostnames parameter for the Oracle - Provision Data Guard v3 and Oracle - Create Data Guard Broker Configuration deployments.</i>	required	Comma-separated list of primary database server host names or IP addresses. If more than one IP address/hostname is entered, it indicates that the primary database is on RAC.
RedoTransmit	TRANSPORT-ON	optional	Start or stop the redo transport services from the primary database to all standby databases. Valid values TRANSPORT-ON or TRANSPORT-OFF.
Standby DB State	APPLY-ON	optional	Start or stop the Redo Apply services on the specified physical standby database. Valid values are APPLY-ON or APPLY-OFF. If you specify the Standby DB State, you must also specify the Standby DB Unique Name.
Standby DB Unique Name		optional	Unique name of the standby database whose property is being changed (see Standby DB State, Archive Lag Target).
Standby Node Hostnames	dma-rac3.mycompany.com, dma-rac4.mycompany.com <i>Use the same value(s) as the Standby Node Hostnames parameter for the Oracle - Provision Data Guard v3 and Oracle - Create Data Guard Broker Configuration deployments.</i>	required	Comma-separated list of up to 30 standby database server host names or IP addresses. If more than one IP address/hostname is entered, it indicates that the standby database is on RAC.

Oracle - Data Guard Broker Switchover

This workflow enables you to perform a Data Guard Broker switchover which will flip the roles of standby and primary databases on an existing Oracle 11.2 (or later) Data Guard configuration.

This workflow is designed to run in an Oracle 11.2 (or later) database environment where Oracle Data Guard has been provisioned and Data Guard Configuration has been set up. It is currently supported on Oracle-supported Linux and AIX platforms.

To use this workflow in your environment, see the following information:

Topic	Information Included
"Prerequisites for this Workflow" on the next page	List of prerequisites that must be satisfied before you can run this workflow
"How this Workflow Works" on page 491	Information about what the workflow does, including validation checks performed, steps executed, and step descriptions
"How to Run this Workflow" on page 492	Instructions for running this workflow in your environment
"Parameters for Oracle - Data Guard Broker Switchover" on page 494	List of input parameters for this workflow

Tip: To patch Server Automation Grid standalone environments, see *Achieve Patch Related Compliance for Oracle Grid Standalone Environments Using DMA*.

To patch more complex Oracle clustered environments, see *Achieve Patch Related Compliance for Oracle RAC Environments Using DMA*.

These documents are available at: <https://softwaresupport.hpe.com/>.

Prerequisites for this Workflow

Before performing the procedures in this section, your environment must meet the following minimum requirements:

- DMA version 10.50.001.000 (or later) with the Advanced Database Provisioning Solution Pack installed
- Servers running one of the following operating systems:
 - Linux (any version that is supported by Oracle and DMA)
 - AIX
 - Solaris

- Oracle 11.2.0.x or 12.1.0.x with the following Oracle configuration:

The Oracle Grid Infrastructure is installed on both the primary cluster servers and the standby cluster servers.

The Oracle database software is installed on all cluster servers.

Your primary database and your primary cluster already exist.

Tip: The following DMA workflows can help you achieve this configuration:

DMAOracle - Provision or Upgrade Grid Infrastructure

DMAOracle - Provision Database Software

DMAOracle - Provision Database

- The primary node of the primary cluster is able to `ssh` as root to ALL nodes in the standby cluster.
- Licenses for Oracle Database and DMA.
- This workflow requires Oracle Database Enterprise Edition version 11.2 (or later). It assumes that the primary database is already provisioned and running and the standby host is available with an RDBMS ORACLE_HOME provisioned. These can be met with workflows Provision Oracle Home and Provision an Oracle Database.
- This workflow also requires root and oracle user ID equivalence across all primary and standby database servers represented in the Data Guard setup. This workflow will regenerate the RSA keys for the Oracle user, setup passwordless SSH login, and add the details of all nodes on all the nodes in `/etc/hosts` file.

Tip: If you are configuring data guard in an Oracle Grid standalone environment, the prerequisites are appropriately simplified. For detailed instructions to provision this environment, see

Standardize Oracle Grid Standalone Provisioning Using DMA, available at
<https://softwaresupport.hpe.com/>

For more information about prerequisites for Oracle database, refer to the [Oracle Server Documentation](#).

How this Workflow Works

This workflow performs the following actions:

Enables you to perform a Data Guard Broker switchover which will flip the roles of standby and primary databases on an existing Oracle 11.2 (or later) Data Guard configuration.

This section instructs you to run this workflow two times.

1. First time describes how to test switchover by switching the database from primary to standby.
2. Second time describes how to revert the switchover by switching the database back from standby to primary.

Steps Executed by the Workflow

The Oracle - Data Guard Broker Switchover workflow includes the following steps. Each step must complete successfully before the next step can start. If a step fails, the workflow reports a failure and all subsequent steps are skipped.

Steps Used by Oracle - Data Guard Broker Switchover

Workflow Step	Description
Gather Parameters for Data Guard Broker Switchover	This step gathers all required input parameters needed for this workflow.
Validate Data Guard Broker Switchover	This step validates the input parameters required for data guard broker switchover.
Perform Data Guard Switchover v2	This step performs a data guard switchover operation in an existing data guard broker configuration.

Note: For input parameter descriptions and defaults, see ["Parameters for Oracle - Data Guard Broker Switchover" on page 494](#)

How to Run this Workflow

The following instructions show you how to customize and run the Oracle - Data Guard Broker Switchover workflow in your environment.

The workflow provides default values for some parameters. These default values are usually sufficient for a "typical" installation. You can override the defaults by specifying parameter values in the deployment. You can also expose additional parameters in the workflow, if necessary, to accomplish more advanced scenarios. Any parameters not explicitly specified in the deployment will have the default values listed in ["Parameters for Oracle - Data Guard Broker Switchover" on page 494](#).

Note: Before following this procedure, review the ["Prerequisites for this Workflow" on page 489](#), and ensure that all requirements are satisfied.

To use the Oracle - Configure Data Guard Broker Properties:

1. Create a deployable copy of the workflow.
2. Determine the values that you will specify for the parameters.

Note: There are no mandatory parameters required to run this workflow. All parameters are optional. You may need to expose additional parameters depending on your objectives.

See ["Parameters for Oracle - Data Guard Broker Switchover" on page 494](#) for detailed descriptions of all input parameters for this workflow, including default values.

3. In the workflow editor, expose any additional parameters that you need. You will specify values for those parameters when you create the deployment or at runtime.
4. Save the changes to the workflow (click **Save** in the lower right corner).
5. Create a new deployment.
6. On the Parameters tab, specify values (or set the type to Runtime Value) for the required parameters listed in step 2 and any additional parameters that you have exposed. You do not need to specify values for those parameters whose default values are appropriate for your environment.
7. On the Targets tab, specify one or more targets for this deployment.
8. Save the deployment (click **Save** in the lower right corner).
9. Run the workflow using this deployment, specifying any runtime parameters.

To verify the results:

The workflow will complete and report SUCCESS on the Console if it has run successfully. If an error occurs during workflow execution, the error is logged, and the workflow terminates in the FAILURE state. The database will be removed from the DMA environment section upon SUCCESS as well.

Parameters for Oracle - Data Guard Broker Switchover

The following tables describe the required and optional input parameters for this workflow. Some of these parameters may not be initially visible in a deployment. For some parameters, if you do not specify a value for a parameter, a default value is assigned.

Parameters for switching the database from primary to standby

Input Parameters Defined in this Step: Gather Parameters for Data Guard Broker Switchover

Parameter Name	Example Value	Required	Description
Oracle Account	oracle	required	The user who owns ORACLE_HOME.
Oracle sys Password	●●●	required	SYS Password for the primary and secondary databases.
Primary Node Hostnames	dma-rac1.mycompany.com, dma-rac2.mycompany.com <i>Use the same value(s) as the Primary Node Hostnames parameter for the Oracle - Provision Data Guard v3, Oracle - Create Data Guard Broker Configuration, and Oracle - Configure Data Guard Broker Properties deployments.</i>	required	Comma-separated list of primary database server host names or IP addresses. If more than one IP address/hostname is entered, it indicates that the primary database is on RAC.
Standby Node Hostnames	dma-rac3.mycompany.com, dma-rac4.mycompany.com <i>Use the same value(s) as the Standby Node Hostnames parameter for the Oracle - Provision Data Guard v3, Oracle - Create Data Guard Broker Configuration, and Oracle - Configure Data Guard Broker Properties deployments.</i>	required	Comma-separated list of up to 30 standby database server host names or IP addresses. If more than one IP address/hostname is entered, it indicates that the standby database is on RAC.
Switchover DB Unique Name	DRorca <i>Use same value as the Standby Connect Identifier for the Oracle - Create Data Guard Broker Configuration deployment.</i>	required	Required if the Switchover or Failover task is specified: Unique name of the standby database that will become the primary database in a switchover or failover operation.

Parameters for switching the database back from standby to primary

Input Parameters Defined in this Step: Gather Parameters for Data Guard Broker Switchover

Parameter Name	Example Value	Required	Description
Oracle Account	oracle	required	The user who owns ORACLE_HOME.
Oracle sys Password	●●●	required	SYS Password for the primary and secondary databases.
Primary Node Hostnames	dma-rac3.mycompany.com, dma-rac4.mycompany.com <i>To switch back to the standby database, use the same value(s) as the Standby Node Hostnames parameter for the Oracle - Provision Data Guard v3, Oracle - Create Data Guard Broker Configuration, and Oracle - Configure Data Guard Broker Properties deployments.</i>	required	Comma-separated list of primary database server host names or IP addresses. If more than one IP address/hostname is entered, it indicates that the primary database is on RAC.
Standby Node Hostnames	dma-rac1.mycompany.com, dma-rac2.mycompany.com <i>To switch back to the primary database, use the same value(s) as the Primary Node Hostnames parameter for the Oracle - Provision Data Guard v3, Oracle - Create Data Guard Broker Configuration, and Oracle - Configure Data Guard Broker Properties deployments.</i>	required	Comma-separated list of up to 30 standby database server host names or IP addresses. If more than one IP address/hostname is entered, it indicates that the standby database is on RAC.
Switchover DB Unique Name	orca <i>Use the primary target's database name.</i>	required	Required if the Switchover or Failover task is specified: Unique name of the standby database that will become the primary database in a switchover or failover operation.

Provisioning Grid Infrastructure

This section describes how to use Database and Middleware Automation (DMA) to create a repeatable, standardized “gold image” for provisioning an Oracle Grid Infrastructure for a standalone server (also known as an Oracle Restart), the Oracle Database software, and then an Oracle database. The following provisioning workflows are available:

- ["Oracle - Provision or Upgrade Grid Infrastructure" on page 524](#)
- ["Oracle - Provision Database Software v2" on page 533](#)
- ["Oracle - Provision Database v3" on page 541](#)

What Oracle Grid standalone does

The Oracle Grid standalone server software allows an Oracle database to use Automatic Storage Management (ASM) local or remote storage. It enables the user to use these features of Oracle 11gR2 Oracle Restart:

- Start automatically with the server
- Manage the configuration and restart the database

Oracle - Provision or Upgrade Grid Infrastructure

This workflow installs Oracle Grid Infrastructure for a Standalone Server or for a Clustered environment. Once provisioned, the installed Grid Infrastructure provides the following:

- Oracle Cluster services (SCAN, VIPs, etc.)
- Oracle Restart services
- The Oracle Listener
- ASM storage to databases provisioned on the server

This workflow is designed to run for Oracle 11.2.0.x and 12.1.0.x. It is currently supported on Oracle-supported Linux, Solaris, and AIX platforms.

To use this workflow in your environment, see the following information:

Topic	Information Included
"Prerequisites for this Workflow" on page 525	List of prerequisites that must be satisfied before you can run this workflow
"How this Workflow Works" on page 526	Information about what the workflow does, including validation checks performed, steps executed, and step descriptions
"How to Run this Workflow" on page 528	Instructions for running this workflow in your environment
"Parameters for Oracle - Provision or Upgrade Grid Infrastructure" on page 530	List of input parameters for this workflow

Prerequisites for this Workflow

Before performing the procedures in this section, your environment must meet the following minimum requirements:

- A server running one of the following operating systems:

Linux (any version that is supported by Oracle and DMA)

AIX

Solaris

This server must meet the Oracle requirements for installing 12c (see [Oracle Database Online Documentation 12c Release 1 \(12.1\)](#) for more information).

- A raw disk (or disks) available to be mounted and used by Oracle ASM. The device cannot be formatted, but it may be partitioned.

- Storage:

A staging directory with 8 gigabytes available to unzip the Oracle Grid Infrastructure and Oracle Database binaries.

For ASM disks, a minimum of 5 gigabytes combined for logical storage (more may be required for your environment).

A minimum of 30 gigabytes on the partition to install Oracle Grid Infrastructure and Oracle Database Homes (more may be required for your environment).

- Licenses for Oracle Database and DMA.

For more information about prerequisites for Oracle database, refer to the [Oracle Server Documentation](#).

How this Workflow Works

This workflow performs the following actions:

Installs Oracle Grid Infrastructure for a Standalone Server or for a Clustered environment.

Steps Executed by the Workflow

The Oracle - Provision or Upgrade Grid Infrastructure workflow includes the following steps. Each step must complete successfully before the next step can start. If a step fails, the workflow reports a failure and all subsequent steps are skipped.

Steps Used by Oracle - Provision or Upgrade Grid Infrastructure

Workflow Step	Description
Gather Parameters for Provision Grid Infrastructure	This step gathers and validates the parameters for the Provision Oracle Grid Infrastructure workflow.
Gather Advanced Parameters for Provision Grid Infrastructure	This step gathers and validates the advanced parameters for the Provision Grid Infrastructure workflow.
Parse Oracle Inventory	<p>This step parses the Oracle inventory files that exists, or else it forwards the inventory information.</p> <ul style="list-style-type: none"> • If the inventory pointer files are specified and exist, parse these files extracting the contents. • If an inventory file is specified and does not exist, ensure a valid specification. • If no inventory file is specified, assign the appropriate default.
Validate Provision Oracle Grid Infrastructure Parameters v2	This step gathers and validates the parameters for the Provision Oracle Grid Infrastructure for Standalone Server workflow.
Decompress Archive Files v2	This step unzips the "zip" archives or gunzip/unarchive cpio.gz files.
Download Software	This step automates the transfer of files from the HP SA Software Library to individual managed servers for use in downstream workflow steps. Verifies checksum of each file transferred.
Verify Oracle Install Software	This step verifies the Oracle Software by locating the installer (runInstaller), the product inventory (products.xml), the default response files, and the rootpre.sh script.
Clean Failed Oracle Grid Infrastructure Install	This step removes files and archives that were downloaded to the target system during previous workflow steps.
Execute Oracle Root Pre Script	This step runs the rootpre.sh script in silent mode - if it exists.
Cleanup Downloaded Files v2	This step removes files and archives that were downloaded to the target system during previous workflow steps.

Steps Used by Oracle - Provision or Upgrade Grid Infrastructure, continued

Workflow Step	Description
Run Oracle Grid Infrastructure Pre-Installation Check	This step runs the runcluvfy.sh script found in the CRS installer directory.
Verify Oracle Grid Infrastructure Response File v2	This step creates or verifies a response file to silently install Grid Infrastructure for Standalone Server. If the response file is not specified, a generic response file is created.
Install Oracle Grid Infrastructure	This step runs the Grid installer in silent mode using the supplied response file.
Run Oracle Grid Root Post Install Commands v2	This step runs a series of commands as the root user as specified by the Grid silent install output.
Run Oracle Grid Post Install Commands v2	This step runs a series of commands as the root user as specified by the Grid silent install output.
Verify Grid Infrastructure Installation Complete	This step will verify the grid services are online and running if response file was not given CRS_SWONLY parameter. Also will login to ASM and verify the disk group was created and online ready for database.
Discover Oracle Databases	<p>This step audits the server's physical environment looking for Oracle instances and databases.</p> <p>Note: Discovery is ONLY additive. It will not remove instances or databases currently in your environment. It is the end-user's responsibility to delete content that is no longer in use.</p> <p>In cluster situations where one node is active while other nodes are inactive, Discovery will only find instances and databases on the active node. Nothing will be added to inactive nodes.</p>
Cleanup Downloaded Files v2	This step removes files and archives that were downloaded to the target system during previous workflow steps.

Note: For input parameter descriptions and defaults, see ["Parameters for Oracle - Provision or Upgrade Grid Infrastructure" on page 530](#).

How to Run this Workflow

The following instructions show you how to customize and run the Oracle - Provision or Upgrade Grid Infrastructure workflow in your environment.

The workflow provides default values for some parameters. These default values are usually sufficient for a "typical" installation. You can override the defaults by specifying parameter values in the deployment. You can also expose additional parameters in the workflow, if necessary, to accomplish more advanced scenarios. Any parameters not explicitly specified in the deployment will have the default values listed in ["Parameters for Oracle - Provision or Upgrade Grid Infrastructure" on page 530](#).

Note: Before following this procedure, review the ["Prerequisites for this Workflow" on page 525](#), and ensure that all requirements are satisfied.

To use the Oracle - Provision or Upgrade Grid Infrastructure workflow:

1. Create a deployable copy of the workflow.
2. Determine the values that you will specify for the parameters.

Note: There are no mandatory parameters required to run this workflow. All parameters are optional. You may need to expose additional parameters depending on your objectives.

See ["Parameters for Oracle - Provision or Upgrade Grid Infrastructure" on page 530](#) for detailed descriptions of all input parameters for this workflow, including default values.

3. In the workflow editor, expose any additional parameters that you need. You will specify values for those parameters when you create the deployment or at runtime.
4. Save the changes to the workflow (click **Save** in the lower right corner).
5. Create a new deployment.
6. On the Parameters tab, specify values (or set the type to Runtime Value) for the required parameters listed in step 2 and any additional parameters that you have exposed. You do not need to specify values for those parameters whose default values are appropriate for your environment.
7. On the Targets tab, specify one or more targets for this deployment.
8. Save the deployment (click **Save** in the lower right corner).
9. Run the workflow using this deployment, specifying any runtime parameters.

To verify the results:

The workflow will complete and report SUCCESS on the Console if it has run successfully. If an error occurs during workflow execution, the error is logged, and the workflow terminates in the FAILURE state. The database will be removed from the DMA environment section upon SUCCESS as well.

Parameters for Oracle - Provision or Upgrade Grid Infrastructure

The following tables describe the required and optional input parameters for this workflow. Some of these parameters may not be initially visible in a deployment. For some parameters, if you do not specify a value for a parameter, a default value is assigned.

Input Parameters Defined in this Step: Gather Parameters for Provision Grid Infrastructure

Parameter Name	Example Value	Required	Description
ASM Diskgroup List	ASMDATA(/dev/raw/raw1)	optional	A comma-separated list of the diskgroups that you are creating, with each diskgroup containing a comma-separated list of its associated disks.
ASM Groups	oinstall:dba:oinstall	required	The operating system groups that manage ASM. The syntax is: ASMGroup:ASMDBA:ASMOper
ASM Password	●●●	required	The password for provisioning an Oracle database using ASM storage. The default is Manager1.
CRS Base	/u01/app/grid	required	The location of the Oracle Base directory. This is where the admin directory is located.
CRS Home	/u01/app/oracle/product/12.1.0/grid1	required	The location where the CRS software will be installed. The default is: /u01/app/oracle/product/12.1.0/grid1
Oracle Software	linuxamd64_12c_grid_1of2.zip, linuxamd64_12c_grid_2of2.zip	required	A comma-separated list of the Oracle Database software (CRS) archive files (.zip or .cpio.gz). ¹

Input Parameters Defined in this Step: Gather Advanced Parameters for Provision Grid Infrastructure

Parameter Name	Example Value	Required	Description
ASM au_size	?	optional	The allocation unit size of the ASM disk group. Valid values are: 1, 2, 4, 8, 16, 32, or 64 (MB). The default is 1.
ASM Disk String	?	optional	Value ASM will use to discover the possible ASM Disks

¹ If the files are not found on the target servers, they will be downloaded from the software repository.

Input Parameters Defined in this Step: Gather Advanced Parameters for Provision Grid Infrastructure, continued

Parameter Name	Example Value	Required	Description
ASM Redundancy	?	optional	The redundancy level of the ASM disk group. Can be one of the following values: EXTERNAL for configuring at least 1 ASM disk, NORMAL for configuring at least 3 ASM disks, and HIGH for at least 5 ASM disks. Will be defaulted to EXTERNAL
Cleanup On Failure	True	optional	Indicates whether to remove downloaded and extracted files—to clean up the installation directory—in the event of workflow failure. Valid values are True and False. The default is True, which will clean up on failure.
Cleanup On Success	True	optional	Indicates whether to remove downloaded and extracted files—to clean up the installation directory—in the event of workflow success. Valid values are True and False. The default is True, which will clean up on success.
CLUSTER - Grid Node List		optional	A comma-separated list of the Grid Infrastructure nodes. Must be in the format: node1-public:node1-private:node1-virtual, node2-public:node2-private:node2-virtual
CLUSTER - Scan Info		optional	The Oracle single Client Access name and port that you will use to reference this cluster without specifying a specific node.
CRS Group	oinstall	required	The system group to be used by the CRS installation. Must be the primary group of the CRS Account User. Typically "oinstall".
CRS Home Name	OraCRS11gR2	required	The unique Oracle name for this CRS software install. Must contain only letters, numbers, and underscores (_).
CRS Name	GRID01	required	The unique Oracle name for this CRS cluster. Must contain only letters, numbers, and dashes (-). The default is RAC01
CRS Response File	?	required	An OUI (Oracle Universal Installer) response file for this CRS installation to be downloaded from the software repository. If not specified, a default will be created by the workflow for the installation based on a default template. It will be deleted upon completion.
CRS User	oracle	required	The user who will own the CRS software. Typically oracle.
Download Location	/tmp	required	The location where the CRS archive has been (or will be) downloaded.
Extract Location	/tmp	required	The directory location where the CRS archive has been (or will be) extracted.

Input Parameters Defined in this Step: Gather Advanced Parameters for Provision Grid Infrastructure, continued

Parameter Name	Example Value	Required	Description
Ignore System Prerequisites	?	optional	Set to Y to include the -ignoreSysPrereqs parameter when running the install. Valid values are Y, N, and blank. Blank defaults to N.
Inventory File	/etc/oraInst.loc	required	The location of the system's current Oracle inventory file. If it does not exist, it will be created.
Listener	LISTENER:1521	optional	Name and port information of the listener. The syntax is Name:Port. The default is LISTENER:1521.
Network Admin Files	?	optional	Comma-delimited list of files to be downloaded and placed in the CRS_HOME/network/admin directory after the Oracle Software is installed.
OCR Devices	+DATA	required	Required: The devices CRS uses to store cluster and database configuration information. The device must have the CRS group, be owned by root, and be at least 256Mb. Must be in the same location as Voting Devices.
runInstaller Parameters	-ignoreSysPrereqs	optional	The parameters to pass to the Oracle runInstaller command. For example: -force or -ignoreSysPrereqs
Trust SSL Certificates			Deprecated: DMA no longer uses this workflow parameter to determine whether the workflow will trust any Secure Sockets Layer (SSL) certificate used to connect to the DMA web server. DMA now uses the com.hp.dma.conn.trustAllCertificates parameter in the dma.xml file.
Upgrade to Oracle 12	False	optional	Set to True if you are upgrading an existing Oracle 11g Grid Infrastructure to Oracle 12 Grid Infrastructure. The default is False.
Voting Devices	+DATA	required	The devices CRS uses to verify cluster node membership and status. The device must have the CRS owner and group and be at least 256Mb. Must be in the same location as OCR Devices.
Web Service Password	●●●	optional	Password for the DMA Discovery web service API.
Web Service URL	DMA.Url	optional	URL for the discovery web service API.
Web Service User		optional	User who is capable of modifying the managed environment by using the DMA Discovery web service API.

Oracle - Provision Database Software v2

This workflow installs Oracle Database software on a server in the location specified by the Oracle Home parameter. The workflow can be customized to provision an Oracle Standalone, Grid Standalone, or CRS RAC environment.

This workflow installs Oracle Database software on a server using the runInstaller utility supplied by Oracle.

To use this workflow, you must provide the Oracle Database software in one of the following forms:

- A software archive (ZIP or cpio.gz file) that exists on the software repository or on the target machine
- Unarchived files on a CD, DVD, NFS mount, or similar device

If the inventory pointer is not found, it is created.

If you do not provide a response file, a default response file is created from the response files included in the software archive. This default response file will install Oracle Database Standard Edition.

This workflow currently supports Oracle version 10.2.0.x, 11.1.0.x, 11.2.0.x, 12.1.0.x. It is supported on Oracle-supported Linux, Solaris, AIX, and HP-UX platforms.

To use this workflow in your environment, see the following information:

Topic	Information Included
"Prerequisites for this Workflow" on page 534	List of prerequisites that must be satisfied before you can run this workflow
"How this Workflow Works" on page 535	Information about what the workflow does, including validation checks performed, steps executed, and step descriptions
"How to Run this Workflow" on page 537	Instructions for running this workflow in your environment
"Parameters for Oracle - Provision Database Software v2" on page 538	List of input parameters for this workflow

Prerequisites for this Workflow

Before performing the procedures in this section, your environment must meet the following minimum requirements:

- A server running one of the following operating systems:

Linux (any version that is supported by Oracle and DMA)

AIX

Solaris

This server must meet the Oracle requirements for installing 12c (see [Oracle Database Online Documentation 12c Release 1 \(12.1\)](#) for more information).

- A raw disk (or disks) available to be mounted and used by Oracle ASM. The device cannot be formatted, but it may be partitioned.

- Storage:

A staging directory with 8 gigabytes available to unzip the Oracle Grid Infrastructure and Oracle Database binaries.

For ASM disks, a minimum of 5 gigabytes combined for logical storage (more may be required for your environment).

A minimum of 30 gigabytes on the partition to install Oracle Grid Infrastructure and Oracle Database Homes (more may be required for your environment).

- Licenses for Oracle Database and DMA.

For more information about prerequisites for Oracle database, refer to the [Oracle Server Documentation](#).

How this Workflow Works

This workflow performs the following actions:

Installs Oracle Database software on a server in the location specified by the Oracle Home parameter. The workflow can be customized to provision an Oracle Standalone, Grid Standalone, or CRS RAC environment.

Steps Executed by the Workflow

The Oracle - Provision Database Software v2 workflow includes the following steps. Each step must complete successfully before the next step can start. If a step fails, the workflow reports a failure and all subsequent steps are skipped.

Steps Used by Oracle - Provision Database Software v2

Workflow Step	Description
Gather Parameters for Provision Oracle Software	This step validates all parameters needed for the Provision Oracle Software workflow.
Gather Advanced Parameters for Provision Oracle Software v2	This step gathers and validates all advanced parameters needed for the Provision Oracle Software workflow.
Prepare Oracle Server	This step prepares the server wrapper for other steps to use.
Verify Oracle Install Location	This step verifies oraInst.loc file and location and creates if needed.
Parse Oracle Inventory	<p>This step parses the Oracle inventory files that exists, or else it forwards the inventory information.</p> <ul style="list-style-type: none"> • If the inventory pointer files are specified and exist, parse these files extracting the contents. • If an inventory file is specified and does not exist, ensure a valid specification. • If no inventory file is specified, assign the appropriate default.
Validate Provision Oracle Software v2	This step validates all parameters needed for the Provision Oracle Software workflow.
Change File Owner and Group	This step changes the ownership and group of each supplied file. A warning is issued for files that are not found.
Download Software	This step automates the transfer of files from the HP SA Software Library to individual managed servers for use in downstream workflow steps. Verifies checksum of each file transferred.
Setup Standby Redo Logs on Primary Database	This step creates the standby redo logs on the primary database needed for Data Guard to successfully synchronize databases.
Uncompress Archive Files	This step unzips the "zip" archives or gunzip/unarchive cpio.gz files.

Steps Used by Oracle - Provision Database Software v2, continued

Workflow Step	Description
Clean Failed Oracle Software Install	This step removes files and archives that were downloaded to the target system during previous workflow steps.
Verify Oracle Install Software	This step verifies the Oracle Software by locating the installer (runInstaller), the product inventory (products.xml), the default response files, and the rootpre.sh script.
Cleanup Downloaded Files v2	This step removes files and archives that were downloaded to the target system during previous workflow steps.
Create Oracle Home Directories	This step creates the Oracle Home and Oracle Base directories and ensures that they are owned by the Oracle user and are in the specified Oracle group.
Execute Oracle Root Pre Script	This step runs the rootpre.sh script in silent mode - if it exists.
Create Oracle Inventory Pointer	This step creates the oracle inventory pointer file (oralnst.loc) if it does not already exist.
Update Oracle Installer Response	This step updates the provided installer response file or, if one is not provided, creates an installer response file based on a default response file provided by Oracle.
Execute Oracle Software Installer v2	This step installs the Oracle software as defined by the response file.
Execute Oracle Install Root Script	This step runs the root.sh script in silent mode if needed.
Cleanup Downloaded Files v2	This step removes files and archives that were downloaded to the target system during previous workflow steps.
Verify Provision Oracle Software v2	This step verifies the installation of Oracle database software.

Note: For input parameter descriptions and defaults, see ["Parameters for Oracle - Provision Database Software v2" on page 538](#).

How to Run this Workflow

The following instructions show you how to customize and run the Oracle - Provision Database Software v2 workflow in your environment.

The workflow provides default values for some parameters. These default values are usually sufficient for a "typical" installation. You can override the defaults by specifying parameter values in the deployment. You can also expose additional parameters in the workflow, if necessary, to accomplish more advanced scenarios. Any parameters not explicitly specified in the deployment will have the default values listed in ["Parameters for Oracle - Provision Database Software v2" on page 538](#).

Note: Before following this procedure, review the ["Prerequisites for this Workflow" on page 534](#), and ensure that all requirements are satisfied.

To use the Oracle - Provision Database Software v2 workflow:

1. Create a deployable copy of the workflow.
2. Determine the values that you will specify for the parameters.

Note: There are no mandatory parameters required to run this workflow. All parameters are optional. You may need to expose additional parameters depending on your objectives.

See ["Parameters for Oracle - Provision Database Software v2" on page 538](#) for detailed descriptions of all input parameters for this workflow, including default values.

3. In the workflow editor, expose any additional parameters that you need. You will specify values for those parameters when you create the deployment or at runtime.
4. Save the changes to the workflow (click **Save** in the lower right corner).
5. Create a new deployment.
6. On the Parameters tab, specify values (or set the type to Runtime Value) for the required parameters listed in step 2 and any additional parameters that you have exposed. You do not need to specify values for those parameters whose default values are appropriate for your environment.
7. On the Targets tab, specify one or more targets for this deployment.
8. Save the deployment (click **Save** in the lower right corner).
9. Run the workflow using this deployment, specifying any runtime parameters.

To verify the results:

The workflow will complete and report SUCCESS on the Console if it has run successfully. If an error occurs during workflow execution, the error is logged, and the workflow terminates in the FAILURE state. The database will be removed from the DMA environment section upon SUCCESS as well.

Parameters for Oracle - Provision Database Software v2

The following tables describe the required and optional input parameters for this workflow. Some of these parameters may not be initially visible in a deployment. For some parameters, if you do not specify a value for a parameter, a default value is assigned.

Input Parameters Defined in this Step: Gather Parameters for Provision Oracle Software

Parameter Name	Example Value	Required	Description
Oracle Account	Maximum Availability	optional	Required only if inventory does not exist. The Oracle user that will own the Oracle Home.
Oracle Base	/u01/app/oracle	required	The fully-qualified path to the Oracle base directory where the admin directories will be located.
Oracle Home	/u01/app/oracle/product/11.2.0/dbhome_1	required	Fully-qualified path name where the Oracle Home will be created. If the specified directory does not exist, it will be created.
Oracle Software	p10404530_112030_Linux-x86-64_1of7.zip,p10404530_112030_Linux-x86-64_2of7.zip	required	Comma-separated list of relative or fully-qualified path names of the Oracle Database software archive files. If a fully-qualified path name points to a file, that file is expected to be on the target. If a relative path name points to a file, that file will be downloaded from the software repository. If a fully-qualified path name is a directory, the software is expected to be unzipped and ready to be applied.

Input Parameters Defined in this Step: Gather Advanced Parameters for Provision Oracle Software v2

Parameter Name	Example Value	Required	Description
Cleanup On Failure	True	optional	Indicates whether to remove downloaded and extracted files—to clean up the installation directory—in the event of workflow failure. Valid values are True and False. The default is True, which will clean up on failure.
Cleanup On Success	True	optional	Indicates whether to remove downloaded and extracted files—to clean up the installation directory—in the event of workflow success. Valid

Input Parameters Defined in this Step: Gather Advanced Parameters for Provision Oracle Software v2, continued

Parameter Name	Example Value	Required	Description
			values are True and False. The default is True, which will clean up on success.
Cluster Nodes		optional	Optional (required when provisioning a RAC database): Comma-separated list of nodes to install software on. Leave blank for non-clustered environments.
DBA Group	?	optional	The DBA group to use for superuser access to the subsequent Oracle Database (typically dba). If not specified, derived from the Oracle OS user.
Download Location	/tmp	optional	The directory where input files already exist or to which files will be downloaded from the software repository.
Enable DNFS	?	optional	When set to 'True' then the workflow will enable the Direct NFS option as part of the Software Installation.
Extract Location	/tmp	optional	The directory location where the Oracle database software archives will be extracted. It will be cleaned up at end of workflow execution. If not specified, a default will be created.
Install Edition	?	optional	The install edition of the Oracle installation. Valid values are SE or EE. The default is EE.
Install Response	?	optional	Location of the Oracle Universal Installer (OUI) response file.
Inventory Files	?	optional	Comma-separated list of fully-qualified Oracle inventory files. If this parameter is not specified, the workflow looks for the oraInst.loc file in /etc and /var/opt/oracle.
Network Admin Files	?	optional	Comma-delimited list of files to be downloaded and placed in the CRS_HOME/network/admin directory after the Oracle Software is installed.
Operator Group	?	optional	The operator group to use for operator access to the subsequent Oracle Database (typically oper). If this parameter is not specified, it is derived from the Oracle OS user.
Oracle Home Name	?	optional	The Oracle Home name. If not specified, it is randomly generated.
RAC One Node Install	?	optional	Set to true to install Oracle RAC One Node software using the oracle.install.db.isRACOneInstall option. The default is false.

Input Parameters Defined in this Step: Gather Advanced Parameters for Provision Oracle Software v2, continued

Parameter Name	Example Value	Required	Description
runInstaller Parameters	-ignoreSysPrereqs	optional	The parameters to pass to the Oracle runInstaller command. For example: -force or -ignoreSysPrereqs ¹

¹This parameter is hidden by default and must be exposed when you make a copy of the workflow.

Oracle - Provision Database v3

This workflow installs Oracle Database software on a server in the location specified by the Oracle Home parameter. The workflow can be customized to provision an Oracle Standalone, Grid Standalone, or CRS RAC environment.

This workflow installs Oracle Database software on a server using the runInstaller utility supplied by Oracle.

To use this workflow, you must provide the Oracle Database software in one of the following forms:

- A software archive (ZIP or cpio.gz file) that exists on the software repository or on the target machine
- Unarchived files on a CD, DVD, NFS mount, or similar device

If the inventory pointer is not found, it is created.

If you do not provide a response file, a default response file is created from the response files included in the software archive. This default response file will install Oracle Database Standard Edition.

This workflow currently supports Oracle version 10.2.0.x, 11.1.0.x, 11.2.0.x, 12.1.0.x. It is supported on Oracle-supported Linux, Solaris, AIX, and HP-UX platforms.

To use this workflow in your environment, see the following information:

Topic	Information Included
"Prerequisites for this Workflow" on page 542	List of prerequisites that must be satisfied before you can run this workflow
"How this Workflow Works" on page 543	Information about what the workflow does, including validation checks performed, steps executed, and step descriptions
"How to Run this Workflow" on page 546	Instructions for running this workflow in your environment
"Parameters for Oracle - Provision Database v3" on page 547	List of input parameters for this workflow

Prerequisites for this Workflow

Before performing the procedures in this section, your environment must meet the following minimum requirements:

- A server running one of the following operating systems:

Linux (any version that is supported by Oracle and DMA)

AIX

Solaris

This server must meet the Oracle requirements for installing 12c (see [Oracle Database Online Documentation 12c Release 1 \(12.1\)](#) for more information).

- A raw disk (or disks) available to be mounted and used by Oracle ASM. The device cannot be formatted, but it may be partitioned.

- Storage:

A staging directory with 8 gigabytes available to unzip the Oracle Grid Infrastructure and Oracle Database binaries.

For ASM disks, a minimum of 5 gigabytes combined for logical storage (more may be required for your environment).

A minimum of 30 gigabytes on the partition to install Oracle Grid Infrastructure and Oracle Database Homes (more may be required for your environment).

- Licenses for Oracle Database and DMA.
- The ORACLE_HOME has already been installed and is ready for the DBCA to run.

For more information about prerequisites for Oracle database, refer to the [Oracle Server Documentation](#).

How this Workflow Works

This workflow performs the following actions:

Provisions an Oracle database on an Oracle Standalone, Grid Standalone, or CRS RAC environment.

Steps Executed by the Workflow

The Oracle - Provision Database v3 workflow includes the following steps. Each step must complete successfully before the next step can start. If a step fails, the workflow reports a failure and all subsequent steps are skipped.

Steps Used by Oracle - Provision Database v3

Workflow Step	Description
Gather Parameters for Provision Oracle Database v2	This step gathers and validates the parameters for the Provision an Oracle Database workflow.
Gather Advanced Parameters for Provision Oracle Database v4	This step gathers and validates the optional advanced parameters for the Provision an Oracle Database workflow.
Prepare Oracle Call Wrapper	This step prepares the call wrappers needed to become the owner of the Oracle Database software and root. It sets the default values for call wrapper and Oracle OS owner variables used in subsequent workflow steps.
Prepare Oracle Instance	This step prepares the call wrappers needed to become the owner of the Oracle Database software and root. It sets the default values for call wrapper and Oracle OS owner variables used in subsequent workflow steps.
Validate Provision an Oracle Database v4	This step validates the parameters for the Provision an Oracle Database workflow.
Check If Download File Exists	This step is designed to facilitate the complicated methodologies that various companies use to distribute their software bundles for installation.
Verify DBCA Response v2	This step creates or verifies a DBCA response file. If the response file does not exist, a generic response file is created.
Open File Permission	This step opens the file permission to ensure read/write for all.
Download Software	This step automates the transfer of files from the HP SA Software Library to individual managed servers for use in downstream workflow steps. Verifies checksum of each file transferred.
Verify Listener v2	<p>This step verifies the following:</p> <ul style="list-style-type: none"> • The listener is already created • The Oracle version is 11.2.0.1 or above. <p>If CRS is already set up (the listener is already created), subsequent steps that run netca will not be executed.</p>
Run DBCA	This step runs Oracle's Database Configuration Assistant (DBCA) with the supplied response file.

Steps Used by Oracle - Provision Database v3, continued

Workflow Step	Description
Verify NetCA Response v2	This step creates or verifies a NetCA response file. If the response file does not exist, it is created.
Parse DBCA Log	This step parses a DBCA log file to ensure a database was correctly created.
Clean Failed Oracle Database Install	This step removes files and archives that were downloaded to the target system during previous workflow steps.
Run NetCA v2	This step runs Oracle's Net Configuration Assistant (NetCA) with the supplied response file.
Add oratab entry	<p>This step adds a new entry in the /etc/oratab files on each node of a RAC cluster or on the local machine.</p> <p>If Oracle version is higher than 11.2 and CRS Home exists, the whole Add Oratab entry functionality is skipped as Oracle will automatically add the necessary entry to ORATAB file.</p>
Post Database Configuration for Provision Oracle Database	This step performs the Post Database Configuration for the pre-provisioned Oracle Database.
Discover Oracle Databases	<p>This step audits the server's physical environment looking for Oracle instances and databases</p> <p>Note: Discovery is ONLY additive. It will not remove instances or databases currently in your environment. It is the end-user's responsibility to delete content that is no longer in use.</p> <p>In cluster situations where one node is active while other nodes are inactive, Discovery will only find instances and databases on the active node. Nothing will be added to inactive nodes.</p>
Run Latest cpu or psu Script	This step runs the catcpu or catpsu script depending on the latest CPU or PSU installed.
Jan08CPU Database Views	This step recompiles database views on a RAC database as required by the CPU patching process if any patches are applied to the specified ORACLE_HOME.
Start or Stop RAC Database	This step starts or stops a RAC database.
Confirm Views Recompiled	This step confirms that the CPUJan2008 view recompile patch has been properly applied.
RAC Recompile Database Views	This step recompiles database views on a RAC database as required by the CPU patching process.
Recompile Invalid Database Objects	This step recompiles invalid database objects using \${ORACLE_HOME}/rdbms/admin/utlrp.sql.
Start or Stop RAC Database	This step starts or stops a RAC database.

Note: For input parameter descriptions and defaults, see ["Parameters for Oracle - Provision Database v3" on page 547](#).

How to Run this Workflow

The following instructions show you how to customize and run the Oracle - Provision Database v3 workflow in your environment.

The workflow provides default values for some parameters. These default values are usually sufficient for a "typical" installation. You can override the defaults by specifying parameter values in the deployment. You can also expose additional parameters in the workflow, if necessary, to accomplish more advanced scenarios. Any parameters not explicitly specified in the deployment will have the default values listed in ["Parameters for Oracle - Provision Database v3" on page 547](#).

Note: Before following this procedure, review the ["Prerequisites for this Workflow" on page 542](#), and ensure that all requirements are satisfied.

To use the Oracle - Provision Database Software v2 workflow:

1. Create a deployable copy of the workflow.
2. Determine the values that you will specify for the parameters.

Note: There are no mandatory parameters required to run this workflow. All parameters are optional. You may need to expose additional parameters depending on your objectives.

See ["Parameters for Oracle - Provision Database v3" on page 547](#) for detailed descriptions of all input parameters for this workflow, including default values.

3. In the workflow editor, expose any additional parameters that you need. You will specify values for those parameters when you create the deployment or at runtime.
4. Save the changes to the workflow (click **Save** in the lower right corner).
5. Create a new deployment.
6. On the Parameters tab, specify values (or set the type to Runtime Value) for the required parameters listed in step 2 and any additional parameters that you have exposed. You do not need to specify values for those parameters whose default values are appropriate for your environment.
7. On the Targets tab, specify one or more targets for this deployment.
8. Save the deployment (click **Save** in the lower right corner).
9. Run the workflow using this deployment, specifying any runtime parameters.

To verify the results:

The workflow will complete and report SUCCESS on the Console if it has run successfully. If an error occurs during workflow execution, the error is logged, and the workflow terminates in the FAILURE state. The database will be removed from the DMA environment section upon SUCCESS as well.

Parameters for Oracle - Provision Database v3

The following tables describe the required and optional input parameters for this workflow. Some of these parameters may not be initially visible in a deployment. For some parameters, if you do not specify a value for a parameter, a default value is assigned.

Input Parameters Defined in this Step: Gather Parameters for Provision Oracle Database v2

Parameter Name	Example Value	Required	Description
Database Name	orca	required	The name of the database to provision.
Datafile Location	+ASMDATA <i>Use a plus sign (+) followed by the same value as the ASM Diskgroup List parameter for the Oracle - Provision or Upgrade Grid Infrastructure deployment.</i>	required	The database file locations.
Oracle Account	oracle <i>Use the same value specified for the Oracle Account parameter for the Oracle - Provision Database Software deployment.</i>	optional	Required only if inventory does not exist. The Oracle user that will own the Oracle Home.
Oracle Base	/u01/app/oracle/product/12.1.0/dbhome_1 <i>Use the same value specified for the Oracle Base parameter for the Oracle - Provision Database Software deployment.</i>	required	The fully-qualified path to the Oracle base directory where the admin directories are located.
Oracle Home	/u01/app/oracle <i>Use the same value specified for the Oracle Base parameter for the Oracle - Provision Database Software deployment.</i>	optional	The Oracle Home to use if more than one Oracle Home exists in the inventory files.
Trust SSL Certificates			Deprecated: DMA no longer uses this workflow parameter to determine whether the workflow will trust any Secure Sockets Layer (SSL) certificate used to connect to the DMA web server. DMA now uses the <code>com.hp.dma.conn.trustAllCertificates</code> parameter in the <code>dma.xml</code> file.
Web Service Password	●●●	required	Password for the DMA Discovery web service API.
Web	DMA.Url	optional	URL for the discovery web

Input Parameters Defined in this Step: Gather Parameters for Provision Oracle Database v2, continued

Parameter Name	Example Value	Required	Description
Service URL			service API.
Web Service User		optional	User who is capable of modifying the managed environment by using the DMA Discovery web service API.

Input Parameters Defined in this Step: Gather Advanced Parameters for Provision Oracle Database v4

Parameter Name	Example Value	Required	Description
ASM Password	<i>Use the same value specified for the ASM Password parameter for the Oracle - Provision or Upgrade Grid Infrastructure deployment.</i>	optional	Optional (required when provisioning an Oracle database using ASM storage): The password used to manage ASM. ¹
Cleanup On Failure	True	optional	Indicates whether to remove downloaded and extracted files—to clean up the installation directory—in the event of workflow failure. Valid values are True and False. The default is True, which will clean up on failure.
Cleanup On Success	True	optional	Indicates whether to remove downloaded and extracted files—to clean up the installation directory—in the event of workflow success. Valid values are True and False. The default is True, which will clean up on success.
Cluster Nodes		optional	Optional (required when provisioning a RAC database): Comma-separated list of nodes where this database will run. Leave blank for non-clustered environments. True
Container Database	False	optional	Set to 'True' if provisioning a container database in Oracle 12c, set to 'False' otherwise. Default is 'False'.
DBCA Character Set	US7ASCII	optional	Specifies the character set where the first two characters denote the region, third character denotes the number of bits used to represent a character, and the rest of the characters denote the standard character set name.

¹ This parameter is hidden by default and must be exposed when you make a copy of the workflow.

Input Parameters Defined in this Step: Gather Advanced Parameters for Provision Oracle Database v4, continued

Parameter Name	Example Value	Required	Description
DBCA National Character Set	UTF8	optional	European data in UTF8 is usually more compact than in AL16UTF16.
DBCA Password ALL	<password>	optional	If set, this password will be used in the DBCA response file for the oracle.install.db.config.starterdb.password.ALL setting and the remaining DBCA Password inputs will be ignored.
DBCA Password DBSNMP	<password>	optional	When set, EM can use DBSNMP user to monitor the database by accessing the performance stats about the database. The DBSNMP credentials are sometimes referred to as the monitoring credentials.
DBCA Password SYS	<password>	optional	When set, the SYS user can login to the database as a Database Administrator. The SYS user owns all base tables and user-accessible view of the data dictionary (Oracle configuration information).
DBCA Password SYSMAN	<password>	optional	The SYSMAN user represents the Enterprise Manager super administrator account. When the password is set, the EM administrator can create and modify other EM administrator accounts and administer the database instance itself.
DBCA Password SYSTEM	<password>	optional	When set, the SYSTEM user can create additional tables and views that display administrative information, and internal tables and views used by various Oracle options and tools.
DBCA Response File	myresponsefile.rsp	optional	Location of a DBCA response file in the software repository to download. If not specified, a default will be used.
DBCA Template File	filename.dbc	optional	Location of a DBCA template file in the software repository to download. If not specified, a default will be used.
Database Name	orca	optional	Required: The name of the database to provision. Required to set the default value for RAC One Node Service Name.
Inventory Files	filename.loc	optional	Comma-separated list of fully-qualified Oracle inventory files. If this parameter is not specified, the workflow looks for the oraInst.loc file in /etc and /var/opt/oracle.
Listener Configuration	listener.ora	optional	Colon-separated name and port of the Oracle listener for this database. If left blank, the Oracle default of LISTENER:1521 will be used.

Input Parameters Defined in this Step: Gather Advanced Parameters for Provision Oracle Database v4, continued

Parameter Name	Example Value	Required	Description
Local Listener	False	optional	Set to True to ignore any GRID installation listener and any attempt to create a local listener (in the Verify Listener step). If the environment does not include GRID, then the local listener will be created regardless of this setting. Default value is False.
NetCA Response File	filename.rsp	optional	Location of a NetCA response file in the software repository to download. If not specified, a default will be used.
Policy Managed	True False	optional	Set to true if Database is policy managed and set to false if Database is admin managed. The default is false.
RAC One Node	True False	optional	Set to true to provision an Oracle RAC One Node database. The default is false.
RAC One Node Service Name	servicename (dbservice1)	optional	The name of the service to connect to the RAC One Node Database.
Variables File	/tmp	optional	Location of a DBCA variables file in the software repository to download. If not specified, a default will be used.
Archivelog On	True False	optional	<p>Set to True to provision database in ARCHIVELOG mode. Default value is False.</p> <p>If you set the value to True, you must provide valid values for Log Archive Destination and Log Archive Format.</p> <p>If the value is default, you must ensure that the values for Log Archive Destination and Log Archive Format are blank.</p>
Log Archive Destination	L:/u01/arch:enable	optional	Comma separated values specifying archive log destinations in the format <R L>:<location>:<state> where R is Remote Location, L is Local Location, <location> is Destination path, and <state> is alternate, reset, defer or enable.
Log Archive Format	'arch_%t_%s_%r.arc', %t_%s_%r.dbf	optional	String specifying archive log format in the format %s %S, %t %T, %a, %d, %r variables where %s is log sequence number, %S is log sequence number, zero filled, %t is thread number, %T is thread number, zero filled, %a is activation ID, %d is database ID and, %r is resetlogs ID that ensures that all archive log file names are unique.

Provisioning RAC

This section describes how to use Database and Middleware Automation (DMA) to create a repeatable, standardized “gold image” for provisioning an Oracle Grid Cluster Ready Services (CRS), Automatic Storage Management (ASM), and Real Application Clusters (RAC) database. The following provisioning workflows are available:

- ["Oracle - Provision or Upgrade Grid Infrastructure" on the next page](#)
- ["Oracle - Provision Database Software v2" on page 533](#)
- ["Oracle - Provision Database v3" on page 541](#)

What Oracle Grid infrastructure for cluster does

The Oracle Grid infrastructure for cluster allows an Oracle database to participate as a RAC database and use common ASM storage across nodes. It enables the user to use these features:

- Start automatically with the server
- Manage the configurations of the database
- Run Oracle Restart
- Use ASM
- Manage nodes in an Oracle cluster
- Manage virtual IP addresses and SCAN virtual IP addresses

Oracle - Provision or Upgrade Grid Infrastructure

This workflow installs Oracle Grid Infrastructure for a Standalone Server or for a Clustered environment. Once provisioned, the installed Grid Infrastructure provides the following:

- Oracle Cluster services (SCAN, VIPs, etc.)
- Oracle Restart services
- The Oracle Listener
- ASM storage to databases provisioned on the server

This workflow is designed to run for Oracle 11.2.0.x and 12.1.0.x. It is currently supported on Oracle-supported Linux, Solaris, and AIX platforms.

To use this workflow in your environment, see the following information:

Topic	Information Included
"Prerequisites for this Workflow" on the next page	List of prerequisites that must be satisfied before you can run this workflow
"How this Workflow Works" on page 526	Information about what the workflow does, including validation checks performed, steps executed, and step descriptions
" How to Run this Workflow" on page 528	Instructions for running this workflow in your environment
"Parameters for Oracle - Provision or Upgrade Grid Infrastructure" on page 530	List of input parameters for this workflow

Prerequisites for this Workflow

Before performing the procedures in this section, your environment must meet the following minimum requirements:

- A server running one of the following operating systems:

Linux (any version that is supported by Oracle and DMA)

AIX

Solaris

This server must meet the Oracle requirements for installing 12c (see [Oracle Database Online Documentation 12c Release 1 \(12.1\)](#) for more information).

- A raw disk (or disks) available to be mounted and used by Oracle ASM. The device cannot be formatted, but it may be partitioned.

- Storage:

A staging directory with 8 gigabytes available to unzip the Oracle Grid Infrastructure and Oracle Database binaries.

For ASM disks, a minimum of 5 gigabytes combined for logical storage (more may be required for your environment).

A minimum of 30 gigabytes on the partition to install Oracle Grid Infrastructure and Oracle Database Homes (more may be required for your environment).

- Licenses for Oracle Database and DMA.

For more information about prerequisites for Oracle database, refer to the [Oracle Server Documentation](#).

How this Workflow Works

This workflow performs the following actions:

Installs Oracle Grid Infrastructure for a Standalone Server or for a Clustered environment.

Steps Executed by the Workflow

The Oracle - Provision or Upgrade Grid Infrastructure workflow includes the following steps. Each step must complete successfully before the next step can start. If a step fails, the workflow reports a failure and all subsequent steps are skipped.

Steps Used by Oracle - Provision or Upgrade Grid Infrastructure

Workflow Step	Description
Gather Parameters for Provision Grid Infrastructure	This step gathers and validates the parameters for the Provision Oracle Grid Infrastructure workflow.
Gather Advanced Parameters for Provision Grid Infrastructure	This step gathers and validates the advanced parameters for the Provision Grid Infrastructure workflow.
Parse Oracle Inventory	<p>This step parses the Oracle inventory files that exists, or else it forwards the inventory information.</p> <ul style="list-style-type: none"> • If the inventory pointer files are specified and exist, parse these files extracting the contents. • If an inventory file is specified and does not exist, ensure a valid specification. • If no inventory file is specified, assign the appropriate default.
Validate Provision Oracle Grid Infrastructure Parameters v2	This step gathers and validates the parameters for the Provision Oracle Grid Infrastructure for Standalone Server workflow.
Decompress Archive Files v2	This step unzips the "zip" archives or gunzip/unarchive cpio.gz files.
Download Software	This step automates the transfer of files from the HP SA Software Library to individual managed servers for use in downstream workflow steps. Verifies checksum of each file transferred.
Verify Oracle Install Software	This step verifies the Oracle Software by locating the installer (runInstaller), the product inventory (products.xml), the default response files, and the rootpre.sh script.
Clean Failed Oracle Grid Infrastructure Install	This step removes files and archives that were downloaded to the target system during previous workflow steps.
Execute Oracle Root Pre Script	This step runs the rootpre.sh script in silent mode - if it exists.
Cleanup Downloaded Files v2	This step removes files and archives that were downloaded to the target system during previous workflow steps.

Steps Used by Oracle - Provision or Upgrade Grid Infrastructure, continued

Workflow Step	Description
Run Oracle Grid Infrastructure Pre-Installation Check	This step runs the runcluvfy.sh script found in the CRS installer directory.
Verify Oracle Grid Infrastructure Response File v2	This step creates or verifies a response file to silently install Grid Infrastructure for Standalone Server. If the response file is not specified, a generic response file is created.
Install Oracle Grid Infrastructure	This step runs the Grid installer in silent mode using the supplied response file.
Run Oracle Grid Root Post Install Commands v2	This step runs a series of commands as the root user as specified by the Grid silent install output.
Run Oracle Grid Post Install Commands v2	This step runs a series of commands as the root user as specified by the Grid silent install output.
Verify Grid Infrastructure Installation Complete	This step will verify the grid services are online and running if response file was not given CRS_SWONLY parameter. Also will login to ASM and verify the disk group was created and online ready for database.
Discover Oracle Databases	<p>This step audits the server's physical environment looking for Oracle instances and databases.</p> <p>Note: Discovery is ONLY additive. It will not remove instances or databases currently in your environment. It is the end-user's responsibility to delete content that is no longer in use.</p> <p>In cluster situations where one node is active while other nodes are inactive, Discovery will only find instances and databases on the active node. Nothing will be added to inactive nodes.</p>
Cleanup Downloaded Files v2	This step removes files and archives that were downloaded to the target system during previous workflow steps.

Note: For input parameter descriptions and defaults, see ["Parameters for Oracle - Provision or Upgrade Grid Infrastructure" on page 530](#).

How to Run this Workflow

The following instructions show you how to customize and run the Oracle - Provision or Upgrade Grid Infrastructure workflow in your environment.

The workflow provides default values for some parameters. These default values are usually sufficient for a "typical" installation. You can override the defaults by specifying parameter values in the deployment. You can also expose additional parameters in the workflow, if necessary, to accomplish more advanced scenarios. Any parameters not explicitly specified in the deployment will have the default values listed in ["Parameters for Oracle - Provision or Upgrade Grid Infrastructure" on page 530](#).

Note: Before following this procedure, review the ["Prerequisites for this Workflow" on page 525](#), and ensure that all requirements are satisfied.

To use the Oracle - Provision or Upgrade Grid Infrastructure workflow:

1. Create a deployable copy of the workflow.
2. Determine the values that you will specify for the parameters.

Note: There are no mandatory parameters required to run this workflow. All parameters are optional. You may need to expose additional parameters depending on your objectives.

See ["Parameters for Oracle - Provision or Upgrade Grid Infrastructure" on page 530](#) for detailed descriptions of all input parameters for this workflow, including default values.

3. In the workflow editor, expose any additional parameters that you need. You will specify values for those parameters when you create the deployment or at runtime.
4. Save the changes to the workflow (click **Save** in the lower right corner).
5. Create a new deployment.
6. On the Parameters tab, specify values (or set the type to Runtime Value) for the required parameters listed in step 2 and any additional parameters that you have exposed. You do not need to specify values for those parameters whose default values are appropriate for your environment.
7. On the Targets tab, specify one or more targets for this deployment.
8. Save the deployment (click **Save** in the lower right corner).
9. Run the workflow using this deployment, specifying any runtime parameters.

To verify the results:

The workflow will complete and report SUCCESS on the Console if it has run successfully. If an error occurs during workflow execution, the error is logged, and the workflow terminates in the FAILURE state. The database will be removed from the DMA environment section upon SUCCESS as well.

Parameters for Oracle - Provision or Upgrade Grid Infrastructure

The following tables describe the required and optional input parameters for this workflow. Some of these parameters may not be initially visible in a deployment. For some parameters, if you do not specify a value for a parameter, a default value is assigned.

Input Parameters Defined in this Step: Gather Parameters for Provision Grid Infrastructure

Parameter Name	Example Value	Required	Description
ASM Diskgroup List	ASMDATA(/dev/raw/raw1)	optional	A comma-separated list of the diskgroups that you are creating, with each diskgroup containing a comma-separated list of its associated disks.
ASM Groups	oinstall:dba:oinstall	required	The operating system groups that manage ASM. The syntax is: ASMGroup:ASMDBA:ASMOper
ASM Password	●●●	required	The password for provisioning an Oracle database using ASM storage. The default is Manager1.
CRS Base	/u01/app/grid	required	The location of the Oracle Base directory. This is where the admin directory is located.
CRS Home	/u01/app/oracle/product/12.1.0/grid1	required	The location where the CRS software will be installed. The default is: /u01/app/oracle/product/12.1.0/grid1
Oracle Software	linuxamd64_12c_grid_1of2.zip, linuxamd64_12c_grid_2of2.zip	required	A comma-separated list of the Oracle Database software (CRS) archive files (.zip or .cpio.gz). ¹

Input Parameters Defined in this Step: Gather Advanced Parameters for Provision Grid Infrastructure

Parameter Name	Example Value	Required	Description
ASM au_size	?	optional	The allocation unit size of the ASM disk group. Valid values are: 1, 2, 4, 8, 16, 32, or 64 (MB). The default is 1.
ASM Disk String	?	optional	Value ASM will use to discover the possible ASM Disks

¹ If the files are not found on the target servers, they will be downloaded from the software repository.

Input Parameters Defined in this Step: Gather Advanced Parameters for Provision Grid Infrastructure, continued

Parameter Name	Example Value	Required	Description
ASM Redundancy	?	optional	The redundancy level of the ASM disk group. Can be one of the following values: EXTERNAL for configuring at least 1 ASM disk, NORMAL for configuring at least 3 ASM disks, and HIGH for at least 5 ASM disks. Will be defaulted to EXTERNAL
Cleanup On Failure	True	optional	Indicates whether to remove downloaded and extracted files—to clean up the installation directory—in the event of workflow failure. Valid values are True and False. The default is True, which will clean up on failure.
Cleanup On Success	True	optional	Indicates whether to remove downloaded and extracted files—to clean up the installation directory—in the event of workflow success. Valid values are True and False. The default is True, which will clean up on success.
CLUSTER - Grid Node List		optional	A comma-separated list of the Grid Infrastructure nodes. Must be in the format: node1-public:node1-private:node1-virtual, node2-public:node2-private:node2-virtual
CLUSTER - Scan Info		optional	The Oracle single Client Access name and port that you will use to reference this cluster without specifying a specific node.
CRS Group	oinstall	required	The system group to be used by the CRS installation. Must be the primary group of the CRS Account User. Typically "oinstall".
CRS Home Name	OraCRS11gR2	required	The unique Oracle name for this CRS software install. Must contain only letters, numbers, and underscores (_).
CRS Name	GRID01	required	The unique Oracle name for this CRS cluster. Must contain only letters, numbers, and dashes (-). The default is RAC01
CRS Response File	?	required	An OUI (Oracle Universal Installer) response file for this CRS installation to be downloaded from the software repository. If not specified, a default will be created by the workflow for the installation based on a default template. It will be deleted upon completion.
CRS User	oracle	required	The user who will own the CRS software. Typically oracle.
Download Location	/tmp	required	The location where the CRS archive has been (or will be) downloaded.
Extract Location	/tmp	required	The directory location where the CRS archive has been (or will be) extracted.

Input Parameters Defined in this Step: Gather Advanced Parameters for Provision Grid Infrastructure, continued

Parameter Name	Example Value	Required	Description
Ignore System Prerequisites	?	optional	Set to Y to include the -ignoreSysPrereqs parameter when running the install. Valid values are Y, N, and blank. Blank defaults to N.
Inventory File	/etc/oraInst.loc	required	The location of the system's current Oracle inventory file. If it does not exist, it will be created.
Listener	LISTENER:1521	optional	Name and port information of the listener. The syntax is Name:Port. The default is LISTENER:1521.
Network Admin Files	?	optional	Comma-delimited list of files to be downloaded and placed in the CRS_HOME/network/admin directory after the Oracle Software is installed.
OCR Devices	+DATA	required	Required: The devices CRS uses to store cluster and database configuration information. The device must have the CRS group, be owned by root, and be at least 256Mb. Must be in the same location as Voting Devices.
runInstaller Parameters	-ignoreSysPrereqs	optional	The parameters to pass to the Oracle runInstaller command. For example: -force or -ignoreSysPrereqs
Trust SSL Certificates			Deprecated: DMA no longer uses this workflow parameter to determine whether the workflow will trust any Secure Sockets Layer (SSL) certificate used to connect to the DMA web server. DMA now uses the com.hp.dma.conn.trustAllCertificates parameter in the dma.xml file.
Upgrade to Oracle 12	False	optional	Set to True if you are upgrading an existing Oracle 11g Grid Infrastructure to Oracle 12 Grid Infrastructure. The default is False.
Voting Devices	+DATA	required	The devices CRS uses to verify cluster node membership and status. The device must have the CRS owner and group and be at least 256Mb. Must be in the same location as OCR Devices.
Web Service Password	●●●	optional	Password for the DMA Discovery web service API.
Web Service URL	DMA.Url	optional	URL for the discovery web service API.
Web Service User		optional	User who is capable of modifying the managed environment by using the DMA Discovery web service API.

Oracle - Provision Database Software v2

This workflow installs Oracle Database software on a server in the location specified by the Oracle Home parameter. The workflow can be customized to provision an Oracle Standalone, Grid Standalone, or CRS RAC environment.

This workflow installs Oracle Database software on a server using the runInstaller utility supplied by Oracle.

To use this workflow, you must provide the Oracle Database software in one of the following forms:

- A software archive (ZIP or cpio.gz file) that exists on the software repository or on the target machine
- Unarchived files on a CD, DVD, NFS mount, or similar device

If the inventory pointer is not found, it is created.

If you do not provide a response file, a default response file is created from the response files included in the software archive. This default response file will install Oracle Database Standard Edition.

This workflow currently supports Oracle version 10.2.0.x, 11.1.0.x, 11.2.0.x, 12.1.0.x. It is supported on Oracle-supported Linux, Solaris, AIX, and HP-UX platforms.

To use this workflow in your environment, see the following information:

Topic	Information Included
"Prerequisites for this Workflow" on the next page	List of prerequisites that must be satisfied before you can run this workflow
"How this Workflow Works" on page 535	Information about what the workflow does, including validation checks performed, steps executed, and step descriptions
"How to Run this Workflow" on page 537	Instructions for running this workflow in your environment
"Parameters for Oracle - Provision Database Software v2" on page 538	List of input parameters for this workflow

Prerequisites for this Workflow

Before performing the procedures in this section, your environment must meet the following minimum requirements:

- A server running one of the following operating systems:

Linux (any version that is supported by Oracle and DMA)

AIX

Solaris

This server must meet the Oracle requirements for installing 12c (see [Oracle Database Online Documentation 12c Release 1 \(12.1\)](#) for more information).

- A raw disk (or disks) available to be mounted and used by Oracle ASM. The device cannot be formatted, but it may be partitioned.

- Storage:

A staging directory with 8 gigabytes available to unzip the Oracle Grid Infrastructure and Oracle Database binaries.

For ASM disks, a minimum of 5 gigabytes combined for logical storage (more may be required for your environment).

A minimum of 30 gigabytes on the partition to install Oracle Grid Infrastructure and Oracle Database Homes (more may be required for your environment).

- Licenses for Oracle Database and DMA.

For more information about prerequisites for Oracle database, refer to the [Oracle Server Documentation](#).

How this Workflow Works

This workflow performs the following actions:

Installs Oracle Database software on a server in the location specified by the Oracle Home parameter. The workflow can be customized to provision an Oracle Standalone, Grid Standalone, or CRS RAC environment.

Steps Executed by the Workflow

The Oracle - Provision Database Software v2 workflow includes the following steps. Each step must complete successfully before the next step can start. If a step fails, the workflow reports a failure and all subsequent steps are skipped.

Steps Used by Oracle - Provision Database Software v2

Workflow Step	Description
Gather Parameters for Provision Oracle Software	This step validates all parameters needed for the Provision Oracle Software workflow.
Gather Advanced Parameters for Provision Oracle Software v2	This step gathers and validates all advanced parameters needed for the Provision Oracle Software workflow.
Prepare Oracle Server	This step prepares the server wrapper for other steps to use.
Verify Oracle Install Location	This step verifies oraInst.loc file and location and creates if needed.
Parse Oracle Inventory	<p>This step parses the Oracle inventory files that exists, or else it forwards the inventory information.</p> <ul style="list-style-type: none"> • If the inventory pointer files are specified and exist, parse these files extracting the contents. • If an inventory file is specified and does not exist, ensure a valid specification. • If no inventory file is specified, assign the appropriate default.
Validate Provision Oracle Software v2	This step validates all parameters needed for the Provision Oracle Software workflow.
Change File Owner and Group	This step changes the ownership and group of each supplied file. A warning is issued for files that are not found.
Download Software	This step automates the transfer of files from the HP SA Software Library to individual managed servers for use in downstream workflow steps. Verifies checksum of each file transferred.
Setup Standby Redo Logs on Primary Database	This step creates the standby redo logs on the primary database needed for Data Guard to successfully synchronize databases.
Uncompress Archive Files	This step unzips the "zip" archives or gunzip/unarchive cpio.gz files.

Steps Used by Oracle - Provision Database Software v2, continued

Workflow Step	Description
Clean Failed Oracle Software Install	This step removes files and archives that were downloaded to the target system during previous workflow steps.
Verify Oracle Install Software	This step verifies the Oracle Software by locating the installer (runInstaller), the product inventory (products.xml), the default response files, and the rootpre.sh script.
Cleanup Downloaded Files v2	This step removes files and archives that were downloaded to the target system during previous workflow steps.
Create Oracle Home Directories	This step creates the Oracle Home and Oracle Base directories and ensures that they are owned by the Oracle user and are in the specified Oracle group.
Execute Oracle Root Pre Script	This step runs the rootpre.sh script in silent mode - if it exists.
Create Oracle Inventory Pointer	This step creates the oracle inventory pointer file (oralnst.loc) if it does not already exist.
Update Oracle Installer Response	This step updates the provided installer response file or, if one is not provided, creates an installer response file based on a default response file provided by Oracle.
Execute Oracle Software Installer v2	This step installs the Oracle software as defined by the response file.
Execute Oracle Install Root Script	This step runs the root.sh script in silent mode if needed.
Cleanup Downloaded Files v2	This step removes files and archives that were downloaded to the target system during previous workflow steps.
Verify Provision Oracle Software v2	This step verifies the installation of Oracle database software.

Note: For input parameter descriptions and defaults, see ["Parameters for Oracle - Provision Database Software v2" on page 538](#).

How to Run this Workflow

The following instructions show you how to customize and run the Oracle - Provision Database Software v2 workflow in your environment.

The workflow provides default values for some parameters. These default values are usually sufficient for a "typical" installation. You can override the defaults by specifying parameter values in the deployment. You can also expose additional parameters in the workflow, if necessary, to accomplish more advanced scenarios. Any parameters not explicitly specified in the deployment will have the default values listed in ["Parameters for Oracle - Provision Database Software v2" on the next page](#).

Note: Before following this procedure, review the ["Prerequisites for this Workflow" on page 534](#), and ensure that all requirements are satisfied.

To use the Oracle - Provision Database Software v2 workflow:

1. Create a deployable copy of the workflow.
2. Determine the values that you will specify for the parameters.

Note: There are no mandatory parameters required to run this workflow. All parameters are optional. You may need to expose additional parameters depending on your objectives.

See ["Parameters for Oracle - Provision Database Software v2" on the next page](#) for detailed descriptions of all input parameters for this workflow, including default values.

3. In the workflow editor, expose any additional parameters that you need. You will specify values for those parameters when you create the deployment or at runtime.
4. Save the changes to the workflow (click **Save** in the lower right corner).
5. Create a new deployment.
6. On the Parameters tab, specify values (or set the type to Runtime Value) for the required parameters listed in step 2 and any additional parameters that you have exposed. You do not need to specify values for those parameters whose default values are appropriate for your environment.
7. On the Targets tab, specify one or more targets for this deployment.
8. Save the deployment (click **Save** in the lower right corner).
9. Run the workflow using this deployment, specifying any runtime parameters.

To verify the results:

The workflow will complete and report SUCCESS on the Console if it has run successfully. If an error occurs during workflow execution, the error is logged, and the workflow terminates in the FAILURE state. The database will be removed from the DMA environment section upon SUCCESS as well.

Parameters for Oracle - Provision Database Software v2

The following tables describe the required and optional input parameters for this workflow. Some of these parameters may not be initially visible in a deployment. For some parameters, if you do not specify a value for a parameter, a default value is assigned.

Input Parameters Defined in this Step: Gather Parameters for Provision Oracle Software

Parameter Name	Example Value	Required	Description
Oracle Account	Maximum Availability	optional	Required only if inventory does not exist. The Oracle user that will own the Oracle Home.
Oracle Base	/u01/app/oracle	required	The fully-qualified path to the Oracle base directory where the admin directories will be located.
Oracle Home	/u01/app/oracle/product/11.2.0/dbhome_1	required	Fully-qualified path name where the Oracle Home will be created. If the specified directory does not exist, it will be created.
Oracle Software	p10404530_112030_Linux-x86-64_1of7.zip,p10404530_112030_Linux-x86-64_2of7.zip	required	Comma-separated list of relative or fully-qualified path names of the Oracle Database software archive files. If a fully-qualified path name points to a file, that file is expected to be on the target. If a relative path name points to a file, that file will be downloaded from the software repository. If a fully-qualified path name is a directory, the software is expected to be unzipped and ready to be applied.

Input Parameters Defined in this Step: Gather Advanced Parameters for Provision Oracle Software v2

Parameter Name	Example Value	Required	Description
Cleanup On Failure	True	optional	Indicates whether to remove downloaded and extracted files—to clean up the installation directory—in the event of workflow failure. Valid values are True and False. The default is True, which will clean up on failure.
Cleanup On Success	True	optional	Indicates whether to remove downloaded and extracted files—to clean up the installation directory—in the event of workflow success. Valid

Input Parameters Defined in this Step: Gather Advanced Parameters for Provision Oracle Software v2, continued

Parameter Name	Example Value	Required	Description
			values are True and False. The default is True, which will clean up on success.
Cluster Nodes		optional	Optional (required when provisioning a RAC database): Comma-separated list of nodes to install software on. Leave blank for non-clustered environments.
DBA Group	?	optional	The DBA group to use for superuser access to the subsequent Oracle Database (typically dba). If not specified, derived from the Oracle OS user.
Download Location	/tmp	optional	The directory where input files already exist or to which files will be downloaded from the software repository.
Enable DNFS	?	optional	When set to 'True' then the workflow will enable the Direct NFS option as part of the Software Installation.
Extract Location	/tmp	optional	The directory location where the Oracle database software archives will be extracted. It will be cleaned up at end of workflow execution. If not specified, a default will be created.
Install Edition	?	optional	The install edition of the Oracle installation. Valid values are SE or EE. The default is EE.
Install Response	?	optional	Location of the Oracle Universal Installer (OUI) response file.
Inventory Files	?	optional	Comma-separated list of fully-qualified Oracle inventory files. If this parameter is not specified, the workflow looks for the oraInst.loc file in /etc and /var/opt/oracle.
Network Admin Files	?	optional	Comma-delimited list of files to be downloaded and placed in the CRS_HOME/network/admin directory after the Oracle Software is installed.
Operator Group	?	optional	The operator group to use for operator access to the subsequent Oracle Database (typically oper). If this parameter is not specified, it is derived from the Oracle OS user.
Oracle Home Name	?	optional	The Oracle Home name. If not specified, it is randomly generated.
RAC One Node Install	?	optional	Set to true to install Oracle RAC One Node software using the oracle.install.db.isRACOneInstall option. The default is false.

Input Parameters Defined in this Step: Gather Advanced Parameters for Provision Oracle Software v2, continued

Parameter Name	Example Value	Required	Description
runInstaller Parameters	-ignoreSysPrereqs	optional	The parameters to pass to the Oracle runInstaller command. For example: -force or -ignoreSysPrereqs ¹

¹This parameter is hidden by default and must be exposed when you make a copy of the workflow.

Oracle - Provision Database v3

This workflow installs Oracle Database software on a server in the location specified by the Oracle Home parameter. The workflow can be customized to provision an Oracle Standalone, Grid Standalone, or CRS RAC environment.

This workflow installs Oracle Database software on a server using the runInstaller utility supplied by Oracle.

To use this workflow, you must provide the Oracle Database software in one of the following forms:

- A software archive (ZIP or cpio.gz file) that exists on the software repository or on the target machine
- Unarchived files on a CD, DVD, NFS mount, or similar device

If the inventory pointer is not found, it is created.

If you do not provide a response file, a default response file is created from the response files included in the software archive. This default response file will install Oracle Database Standard Edition.

This workflow currently supports Oracle version 10.2.0.x, 11.1.0.x, 11.2.0.x, 12.1.0.x. It is supported on Oracle-supported Linux, Solaris, AIX, and HP-UX platforms.

To use this workflow in your environment, see the following information:

Topic	Information Included
"Prerequisites for this Workflow" on the next page	List of prerequisites that must be satisfied before you can run this workflow
"How this Workflow Works" on page 543	Information about what the workflow does, including validation checks performed, steps executed, and step descriptions
"How to Run this Workflow" on page 546	Instructions for running this workflow in your environment
"Parameters for Oracle - Provision Database v3" on page 547	List of input parameters for this workflow

Prerequisites for this Workflow

Before performing the procedures in this section, your environment must meet the following minimum requirements:

- A server running one of the following operating systems:

Linux (any version that is supported by Oracle and DMA)

AIX

Solaris

This server must meet the Oracle requirements for installing 12c (see [Oracle Database Online Documentation 12c Release 1 \(12.1\)](#) for more information).

- A raw disk (or disks) available to be mounted and used by Oracle ASM. The device cannot be formatted, but it may be partitioned.

- Storage:

A staging directory with 8 gigabytes available to unzip the Oracle Grid Infrastructure and Oracle Database binaries.

For ASM disks, a minimum of 5 gigabytes combined for logical storage (more may be required for your environment).

A minimum of 30 gigabytes on the partition to install Oracle Grid Infrastructure and Oracle Database Homes (more may be required for your environment).

- Licenses for Oracle Database and DMA.
- The ORACLE_HOME has already been installed and is ready for the DBCA to run.

For more information about prerequisites for Oracle database, refer to the [Oracle Server Documentation](#).

How this Workflow Works

This workflow performs the following actions:

Provisions an Oracle database on an Oracle Standalone, Grid Standalone, or CRS RAC environment.

Steps Executed by the Workflow

The Oracle - Provision Database v3 workflow includes the following steps. Each step must complete successfully before the next step can start. If a step fails, the workflow reports a failure and all subsequent steps are skipped.

Steps Used by Oracle - Provision Database v3

Workflow Step	Description
Gather Parameters for Provision Oracle Database v2	This step gathers and validates the parameters for the Provision an Oracle Database workflow.
Gather Advanced Parameters for Provision Oracle Database v4	This step gathers and validates the optional advanced parameters for the Provision an Oracle Database workflow.
Prepare Oracle Call Wrapper	This step prepares the call wrappers needed to become the owner of the Oracle Database software and root. It sets the default values for call wrapper and Oracle OS owner variables used in subsequent workflow steps.
Prepare Oracle Instance	This step prepares the call wrappers needed to become the owner of the Oracle Database software and root. It sets the default values for call wrapper and Oracle OS owner variables used in subsequent workflow steps.
Validate Provision an Oracle Database v4	This step validates the parameters for the Provision an Oracle Database workflow.
Check If Download File Exists	This step is designed to facilitate the complicated methodologies that various companies use to distribute their software bundles for installation.
Verify DBCA Response v2	This step creates or verifies a DBCA response file. If the response file does not exist, a generic response file is created.
Open File Permission	This step opens the file permission to ensure read/write for all.
Download Software	This step automates the transfer of files from the HP SA Software Library to individual managed servers for use in downstream workflow steps. Verifies checksum of each file transferred.
Verify Listener v2	<p>This step verifies the following:</p> <ul style="list-style-type: none"> • The listener is already created • The Oracle version is 11.2.0.1 or above. <p>If CRS is already set up (the listener is already created), subsequent steps that run netca will not be executed.</p>
Run DBCA	This step runs Oracle's Database Configuration Assistant (DBCA) with the supplied response file.

Steps Used by Oracle - Provision Database v3, continued

Workflow Step	Description
Verify NetCA Response v2	This step creates or verifies a NetCA response file. If the response file does not exist, it is created.
Parse DBCA Log	This step parses a DBCA log file to ensure a database was correctly created.
Clean Failed Oracle Database Install	This step removes files and archives that were downloaded to the target system during previous workflow steps.
Run NetCA v2	This step runs Oracle's Net Configuration Assistant (NetCA) with the supplied response file.
Add oratab entry	<p>This step adds a new entry in the /etc/oratab files on each node of a RAC cluster or on the local machine.</p> <p>If Oracle version is higher than 11.2 and CRS Home exists, the whole Add Oratab entry functionality is skipped as Oracle will automatically add the necessary entry to ORATAB file.</p>
Post Database Configuration for Provision Oracle Database	This step performs the Post Database Configuration for the pre-provisioned Oracle Database.
Discover Oracle Databases	<p>This step audits the server's physical environment looking for Oracle instances and databases</p> <p>Note: Discovery is ONLY additive. It will not remove instances or databases currently in your environment. It is the end-user's responsibility to delete content that is no longer in use.</p> <p>In cluster situations where one node is active while other nodes are inactive, Discovery will only find instances and databases on the active node. Nothing will be added to inactive nodes.</p>
Run Latest cpu or psu Script	This step runs the catcpu or catpsu script depending on the latest CPU or PSU installed.
Jan08CPU Database Views	This step recompiles database views on a RAC database as required by the CPU patching process if any patches are applied to the specified ORACLE_HOME.
Start or Stop RAC Database	This step starts or stops a RAC database.
Confirm Views Recompiled	This step confirms that the CPUJan2008 view recompile patch has been properly applied.
RAC Recompile Database Views	This step recompiles database views on a RAC database as required by the CPU patching process.
Recompile Invalid Database Objects	This step recompiles invalid database objects using \${ORACLE_HOME}/rdbms/admin/utlrp.sql.
Start or Stop RAC Database	This step starts or stops a RAC database.

Note: For input parameter descriptions and defaults, see "[Parameters for Oracle - Provision Database v3](#)" on page 547.

How to Run this Workflow

The following instructions show you how to customize and run the Oracle - Provision Database v3 workflow in your environment.

The workflow provides default values for some parameters. These default values are usually sufficient for a "typical" installation. You can override the defaults by specifying parameter values in the deployment. You can also expose additional parameters in the workflow, if necessary, to accomplish more advanced scenarios. Any parameters not explicitly specified in the deployment will have the default values listed in ["Parameters for Oracle - Provision Database v3" on the next page](#).

Note: Before following this procedure, review the ["Prerequisites for this Workflow" on page 542](#), and ensure that all requirements are satisfied.

To use the Oracle - Provision Database Software v2 workflow:

1. Create a deployable copy of the workflow.
2. Determine the values that you will specify for the parameters.

Note: There are no mandatory parameters required to run this workflow. All parameters are optional. You may need to expose additional parameters depending on your objectives.

See ["Parameters for Oracle - Provision Database v3" on the next page](#) for detailed descriptions of all input parameters for this workflow, including default values.

3. In the workflow editor, expose any additional parameters that you need. You will specify values for those parameters when you create the deployment or at runtime.
4. Save the changes to the workflow (click **Save** in the lower right corner).
5. Create a new deployment.
6. On the Parameters tab, specify values (or set the type to Runtime Value) for the required parameters listed in step 2 and any additional parameters that you have exposed. You do not need to specify values for those parameters whose default values are appropriate for your environment.
7. On the Targets tab, specify one or more targets for this deployment.
8. Save the deployment (click **Save** in the lower right corner).
9. Run the workflow using this deployment, specifying any runtime parameters.

To verify the results:

The workflow will complete and report SUCCESS on the Console if it has run successfully. If an error occurs during workflow execution, the error is logged, and the workflow terminates in the FAILURE state. The database will be removed from the DMA environment section upon SUCCESS as well.

Parameters for Oracle - Provision Database v3

The following tables describe the required and optional input parameters for this workflow. Some of these parameters may not be initially visible in a deployment. For some parameters, if you do not specify a value for a parameter, a default value is assigned.

Input Parameters Defined in this Step: Gather Parameters for Provision Oracle Database v2

Parameter Name	Example Value	Required	Description
Database Name	orca	required	The name of the database to provision.
Datafile Location	+ASMDATA <i>Use a plus sign (+) followed by the same value as the ASM Diskgroup List parameter for the Oracle - Provision or Upgrade Grid Infrastructure deployment.</i>	required	The database file locations.
Oracle Account	oracle <i>Use the same value specified for the Oracle Account parameter for the Oracle - Provision Database Software deployment.</i>	optional	Required only if inventory does not exist. The Oracle user that will own the Oracle Home.
Oracle Base	/u01/app/oracle/product/12.1.0/dbhome_1 <i>Use the same value specified for the Oracle Base parameter for the Oracle - Provision Database Software deployment.</i>	required	The fully-qualified path to the Oracle base directory where the admin directories are located.
Oracle Home	/u01/app/oracle <i>Use the same value specified for the Oracle Base parameter for the Oracle - Provision Database Software deployment.</i>	optional	The Oracle Home to use if more than one Oracle Home exists in the inventory files.
Trust SSL Certificates			Deprecated: DMA no longer uses this workflow parameter to determine whether the workflow will trust any Secure Sockets Layer (SSL) certificate used to connect to the DMA web server. DMA now uses the <code>com.hp.dma.conn.trustAllCertificates</code> parameter in the <code>dma.xml</code> file.
Web Service Password	●●●	required	Password for the DMA Discovery web service API.
Web	DMA.Url	optional	URL for the discovery web

Input Parameters Defined in this Step: Gather Parameters for Provision Oracle Database v2, continued

Parameter Name	Example Value	Required	Description
Service URL			service API.
Web Service User		optional	User who is capable of modifying the managed environment by using the DMA Discovery web service API.

Input Parameters Defined in this Step: Gather Advanced Parameters for Provision Oracle Database v4

Parameter Name	Example Value	Required	Description
ASM Password	<i>Use the same value specified for the ASM Password parameter for the Oracle - Provision or Upgrade Grid Infrastructure deployment.</i>	optional	Optional (required when provisioning an Oracle database using ASM storage): The password used to manage ASM. ¹
Cleanup On Failure	True	optional	Indicates whether to remove downloaded and extracted files—to clean up the installation directory—in the event of workflow failure. Valid values are True and False. The default is True, which will clean up on failure.
Cleanup On Success	True	optional	Indicates whether to remove downloaded and extracted files—to clean up the installation directory—in the event of workflow success. Valid values are True and False. The default is True, which will clean up on success.
Cluster Nodes		optional	Optional (required when provisioning a RAC database): Comma-separated list of nodes where this database will run. Leave blank for non-clustered environments. True
Container Database	False	optional	Set to 'True' if provisioning a container database in Oracle 12c, set to 'False' otherwise. Default is 'False'.
DBCA Character Set	US7ASCII	optional	Specifies the character set where the first two characters denote the region, third character denotes the number of bits used to represent a character, and the rest of the characters denote the standard character set name.

¹ This parameter is hidden by default and must be exposed when you make a copy of the workflow.

Input Parameters Defined in this Step: Gather Advanced Parameters for Provision Oracle Database v4, continued

Parameter Name	Example Value	Required	Description
DBCA National Character Set	UTF8	optional	European data in UTF8 is usually more compact than in AL16UTF16.
DBCA Password ALL	<password>	optional	If set, this password will be used in the DBCA response file for the oracle.install.db.config.starterdb.password.ALL setting and the remaining DBCA Password inputs will be ignored.
DBCA Password DBSNMP	<password>	optional	When set, EM can use DBSNMP user to monitor the database by accessing the performance stats about the database. The DBSNMP credentials are sometimes referred to as the monitoring credentials.
DBCA Password SYS	<password>	optional	When set, the SYS user can login to the database as a Database Administrator. The SYS user owns all base tables and user-accessible view of the data dictionary (Oracle configuration information).
DBCA Password SYSMAN	<password>	optional	The SYSMAN user represents the Enterprise Manager super administrator account. When the password is set, the EM administrator can create and modify other EM administrator accounts and administer the database instance itself.
DBCA Password SYSTEM	<password>	optional	When set, the SYSTEM user can create additional tables and views that display administrative information, and internal tables and views used by various Oracle options and tools.
DBCA Response File	myresponsefile.rsp	optional	Location of a DBCA response file in the software repository to download. If not specified, a default will be used.
DBCA Template File	filename.dbc	optional	Location of a DBCA template file in the software repository to download. If not specified, a default will be used.
Database Name	orca	optional	Required: The name of the database to provision. Required to set the default value for RAC One Node Service Name.
Inventory Files	filename.loc	optional	Comma-separated list of fully-qualified Oracle inventory files. If this parameter is not specified, the workflow looks for the oraInst.loc file in /etc and /var/opt/oracle.
Listener Configuration	listener.ora	optional	Colon-separated name and port of the Oracle listener for this database. If left blank, the Oracle default of LISTENER:1521 will be used.

Input Parameters Defined in this Step: Gather Advanced Parameters for Provision Oracle Database v4, continued

Parameter Name	Example Value	Required	Description
Local Listener	False	optional	Set to True to ignore any GRID installation listener and any attempt to create a local listener (in the Verify Listener step). If the environment does not include GRID, then the local listener will be created regardless of this setting. Default value is False.
NetCA Response File	filename.rsp	optional	Location of a NetCA response file in the software repository to download. If not specified, a default will be used.
Policy Managed	True False	optional	Set to true if Database is policy managed and set to false if Database is admin managed. The default is false.
RAC One Node	True False	optional	Set to true to provision an Oracle RAC One Node database. The default is false.
RAC One Node Service Name	servicename (dbservice1)	optional	The name of the service to connect to the RAC One Node Database.
Variables File	/tmp	optional	Location of a DBCA variables file in the software repository to download. If not specified, a default will be used.
Archivelog On	True False	optional	<p>Set to True to provision database in ARCHIVELOG mode. Default value is False.</p> <p>If you set the value to True, you must provide valid values for Log Archive Destination and Log Archive Format.</p> <p>If the value is default, you must ensure that the values for Log Archive Destination and Log Archive Format are blank.</p>
Log Archive Destination	L:/u01/arch:enable	optional	Comma separated values specifying archive log destinations in the format <R L>:<location>:<state> where R is Remote Location, L is Local Location, <location> is Destination path, and <state> is alternate, reset, defer or enable.
Log Archive Format	'arch_%t_%s_%r.arc', %t_%s_%r.dbf	optional	String specifying archive log format in the format %s %S, %t %T, %a, %d, %r variables where %s is log sequence number, %S is log sequence number, zero filled, %t is thread number, %T is thread number, zero filled, %a is activation ID, %d is database ID and, %r is resetlogs ID that ensures that all archive log file names are unique.

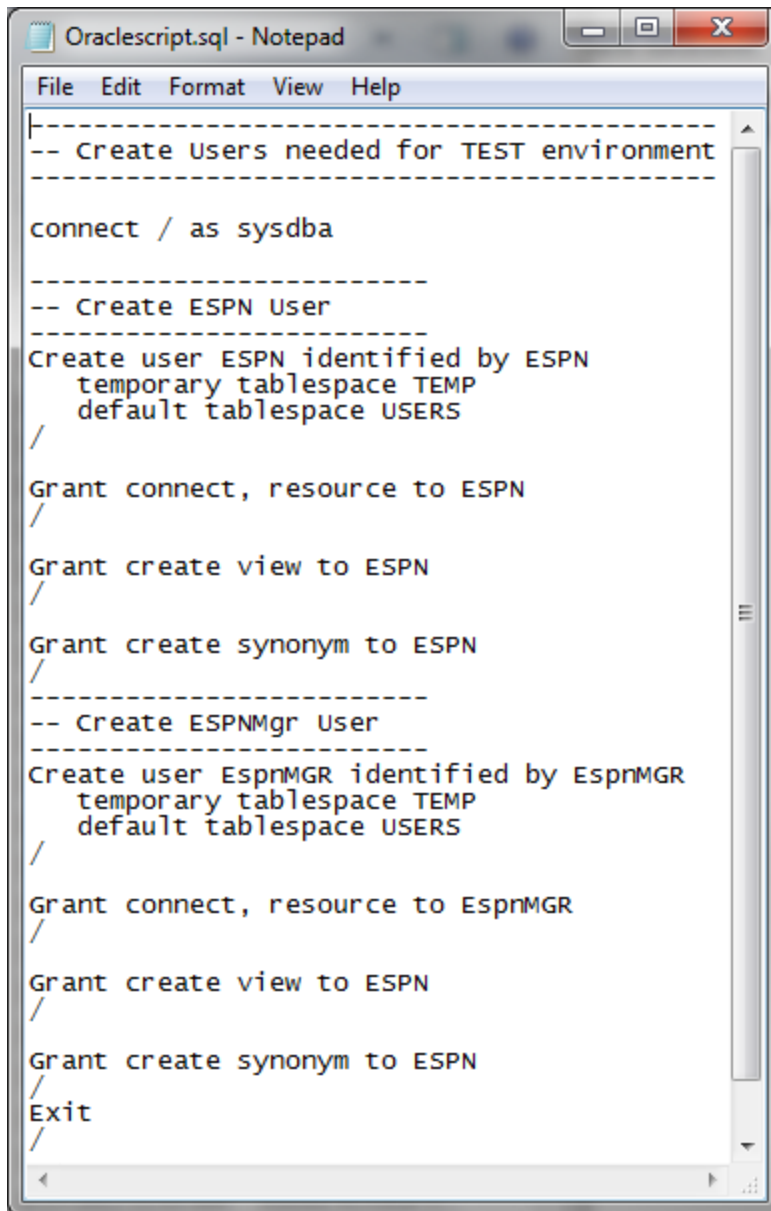
Oracle - SQL Release v3

This workflow deploys and executes an SQL script (or scripts) against target Oracle databases.

This workflow is designed for SQL script and embedded SQL script transactions to be deployed and executed against target Oracle databases. SQL scripts and embedded SQL scripts are stored and downloaded from the software repository .

If the SQL scripts are embedded within an SQL script, this workflow has the ability to download the embedded scripts from SA core. This workflow can download only one level of embedded SQL scripts.

Before running the Oracle - SQL Release workflow you need to create the SQL script file (or files). For example:



```
Oraclescript.sql - Notepad
File Edit Format View Help
-----
-- Create Users needed for TEST environment
-----

connect / as sysdba

-----
-- Create ESPN User
-----
Create user ESPN identified by ESPN
    temporary tablespace TEMP
    default tablespace USERS
/

Grant connect, resource to ESPN
/

Grant create view to ESPN
/

Grant create synonym to ESPN
/

-----
-- Create ESPNMGR User
-----
Create user EspnMGR identified by EspnMGR
    temporary tablespace TEMP
    default tablespace USERS
/

Grant connect, resource to EspnMGR
/

Grant create view to ESPN
/

Grant create synonym to ESPN
/
Exit
/
```

You can customize what the workflow checks in the SQL scripts and embedded SQL scripts:

- Oracle database links
- Oracle system grants based on your list of exceptions
- Prohibited SQL statements based on a regular expression

If all the tests pass, the SQL scripts and embedded SQL scripts will be deployed and executed against the target Oracle databases.

When you create a deployment there is an option to automatically execute a rollback when an error occurs while running the SQL scripts. This rolls back not only the SQL transaction that generated the error but also the previously committed transactions defined within the deployed SQL script.

There is also an option to specify a rollback file that can be executed at a later time. The rollback SQL file serves as an audit file for future use—it records all SQL transactions performed by the SQL scripts and embedded SQL scripts.

Note: This workflow does not provide any pre-parsing of the SQL scripts or embedded SQL scripts.

To use this workflow in your environment, see the following information:

Topic	Information Included
"Prerequisites for this Workflow"	List of prerequisites that must be satisfied before you can run this workflow
"How this Workflow Works"	Information about what the workflow does, including validation checks performed, and steps executed
"How to Run this Workflow"	Instructions for running this workflow in your environment
"Sample Scenarios"	Examples of typical parameter values for this workflow
"Parameters for Oracle - SQL Release v3" on page 566	List of input parameters for this workflow

Prerequisites for this Workflow

Be sure that the following prerequisites are satisfied before you run the "Oracle - SQL Release v3" workflow.

Dependencies

- The latest DMA solution packs require the latest DMA platform. To use the latest solution packs, update the DMA platform. DMA10.50.001.000 solution packs are supported on DMA10.50.001.000 (and later).
- You have installed the Database Compliance solution pack.
- The SQL script must reside on the target server or in the software repository.
- The Oracle instance port must be populated correctly.
- Target servers must be in archive log mode if you desire to execute rollback.
- The target instance has been discovered prior to running this workflow to gather the instance information from the metadata.

Supported Versions of Oracle Database

10gR2 *, 11gR1 *, 11gR2, and 12cR1

* = Out of Oracle standard support

SQL Scripts

You need to create the SQL script file (or files) that manage the release. The files may contain the following Oracle DML and DDL commands:

ALTER INDEX	DELETE	INSERT
CREATE INDEX	DROP INDEX	GRANT PRIVILEGE
CREATE SYNONYM	DROP SYNONYM	REVOKE PRIVILEGE
CREATE VIEW	DROP TABLE	UPDATE
CREATE TABLE	DROP VIEW	
CREATE USER	DROP USER	

Note: Any valid SQL command that is not included in the above table can still be contained in an SQL script, but the workflow's Rollback functionality will not be supported. You need to specify N for the Execute Rollback parameter when you deploy the workflow.

Tip: List the SQL script files in the SQL scripts parameter in the order in which they need to be

executed.

OracleSQL Documentation

For more information about prerequisites for Oracle Database, refer to the [Oracle Database Product Documentation](#).

How this Workflow Works

The following information describes how the "Oracle - SQL Release v3" workflow works.

Overview

The workflow starts by gathering input parameters and constructing commands that will be used in subsequent steps .

If the SQL scripts and embedded SQL scripts does not exist on the specified target location, they are downloaded from the DMA software repository.

Based on the parameters you set when you create your deployment, the workflow will do the following:

- Check the SQL code for Oracle database links—if any are found, the workflow will exit with a failure code.
- Check the SQL code for Oracle system grants specified in the Check System Grants Exception List parameter—if any are found, the workflow will exit with a failure code.
- Check the SQL code for a regular expression specified in the Regular Expression parameter—if it is found, the workflow will exit with a failure code.
- Checks the SQL syntax for errors—if any are found and Check SQL Syntax Ignore Errors is not True, the workflow will exit with a failure code.

If no errors were found (or syntax errors are found and Check SQL Syntax Ignore Errors is True), the workflow creates an SQL*Plus session to run the SQL scripts. Any errors that are on the Acceptable ORA Error list are ignored.

If Execute Rollback is enabled and log archiving is turned on, a rollback SQL script file will be created. If an error occurs during the execution of the SQL scripts a rollback will automatically be performed—as if the SQL scripts had never been executed.

The workflow ends by cleaning up any temporary downloaded files.

Validation Checks Performed

This workflow validates the SQL scripts in the following ways:

1. If you set the Check Database Links Run Flag to Y, the workflow searches for the @ character to indicate a database link—ignoring any @ characters within single quotes.
2. If you set the Check System Grants Run Flag to Y, the workflow searches the SQL statements for the system grants that you specified in the Check System Grants Exception List parameter.

For example:

If you specify CREATE VIEW, the workflow makes sure there are no queries of the form GRANT CREATE VIEW TO myuser.

3. If you set the Check Prohibited Statements Run Flag to Y, the workflow searches the SQL statements for the Regular Expression that you specify.
4. The workflow checks the SQL syntax according to the data type specified in the Check SQL Syntax Database Type parameter. If you set the Check SQL Syntax Ignore Errors to True, any syntax errors will be ignored and the workflow will continue.

If any of the validation checks fail, the workflow will output the offending SQL line to stdout, return an error status, and the SQL scripts will not be executed.

Steps Executed

The "Oracle - SQL Release v3" workflow includes the following steps. Each step must complete successfully before the next step can start. If a step fails, the workflow reports a failure and all subsequent steps are skipped.

Steps Used in Oracle - SQL Release v3

Workflow Step	Description
Gather Parameters for Oracle SQL Release v3	This step accepts the basic input parameters for the workflow. The parameters will be used in subsequent steps. This step also constructs the commands needed to execute subsequent steps in the workflow as either the OS administrative user or the user who owns the pertinent ORACLE_HOME.
Validate Oracle SQL Release v3	This step validates the input parameters for Oracle SQL Release v3.
Check if Download File Exists	This step determines whether one or more specified files already exist on the target server.
Check For Nested SQL files in Oracle SQL file	This step checks for embedded SQL scripts.

Steps Used in Oracle - SQL Release v3, continued

Workflow Step	Description
Download Software	This step downloads a list of files to a specified location on the target server.
Set File Owner and Group Permissions For Oracle SQL files	This step changes the ownership and group of each supplied files. A warning is displayed if any files that are not found in the specified location.
Check Oracle Database Links	This step checks the SQL scripts for the use of database links taking care to exclude hard-coded strings. If any are found the workflow will fail.
Check Oracle System Grants	This step checks an SQL script for any system level grants and for specific privileges specified in the Check System Grants Exception List parameter. If any are found the workflow will fail.
Check Prohibited Statements In SQL Scripts	This step applies a regular expression to each SQL statement in an SQL script. Any regex matches are output to stdout, an error status is returned, and the workflow will fail.
Execute SQL Syntax Check	This step executes an SQL syntax check of the SQL script files. It then reports pass or fail for each file and the number of syntax errors found. If Check SQL Syntax Ignore Errors is set to True, any syntax errors will be ignored and the workflow will continue.
Run Oracle SQL Plus Script v3	<p>This step executes an SQL*Plus Script. It checks the output for any errors. Any errors that are on the Acceptable ORA Error list are ignored.</p> <p>Note: This is designed to be run by the Oracle software owner (typically oracle).</p> <p>If Execute Rollback is enabled, log archiving must be turned on.</p>
Create and Execute Rollback Script	<p>This step creates the rollback SQL script for all actions executed in the SQL release process. If Execute Rollback is enabled and an error occurs during the release process, the step will also execute the rollback SQL script.</p> <p>Note: This step is designed to be run as the Oracle software owner (typically oracle).</p> <p>This step is designed to only work with the Run Oracle SQL*Plus Script step and cannot be used standalone since it depends on the log archiving.</p>
Cleanup Downloaded Files	This step removes all temporary downloaded files and archives.

Note: For input parameter descriptions and defaults, see ["Parameters for Oracle - SQL Release v3" on page 566](#).

How to Run this Workflow

The following instructions show you how to customize and run the ["Oracle - SQL Release v3"](#) workflow in your environment.

Tip: For detailed instructions to run DMA workflows—using the Oracle - Compliance Audit workflow as an example—see DMA Quick Start Tutorial.

The workflow provides default values for some parameters. These default values are usually sufficient for a "typical" installation. You can override the defaults by specifying parameter values in the deployment. You can also expose additional parameters in the workflow, if necessary, to accomplish more advanced scenarios. Any parameters not explicitly specified in the deployment will have the default values listed in ["Parameters for Oracle - SQL Release v3" on page 566](#).

Note: Before following this procedure, review the ["Prerequisites for this Workflow" on page 554](#), and ensure that all requirements are satisfied.

To use the Oracle - SQL Release workflow:

1. Create a deployable copy of the workflow.
2. Determine the values that you will specify for the following parameters:

Input Parameters for Gather Parameters for Oracle SQL Release

Parameter Name	Default Value	Required	Description
Acceptable ORA Error		optional	Comma-separated list of ORA errors that will be expected (and can be ignored) while running release scripts. For example: ORA-00942
Check Database Links Run Flag	Y	required	Flag to indicate whether the workflow should run the database links check. Valid values are Y (run the check) or N (do not run the check).
Regular Expression Check Prohibited Statements Run Flag Check Prohibited Statements Run Flag		optional	The regular expression to be searched for in all of the SQL scripts to be deployed. If the specified regular expression is found, the workflow exits with a failure. For example: drop\s+table will match all statements that drop a table.
Check Prohibited	no default	required	Flag to indicate whether the workflow should run the prohibited statements check. Valid values are Y (run

Input Parameters for Gather Parameters for Oracle SQL Release, continued

Parameter Name	Default Value	Required	Description
Statements Run Flag			the check) or N (do not run the check).
Check SQL Syntax Database Type	dbvoracle	optional	Database type used to set the SQL parser. For example: dbvoracle, dbvsybase, dbvmssql, or dbvdb2. See SQL Parser Documentation for valid options.
Check SQL Syntax Ignore Errors	False	optional	Flag to indicate whether the workflow should pass the SQL syntax check regardless of whether or not syntax errors are found. Valid values are True (the check will always pass) or False (the check will fail if syntax errors are present).
Check System Grants Exception List	CREATE VIEW, CREATE SYNONYM, CREATE CLUSTER, CREATE TABLE	optional	Comma-separated list of system privileges that are not allowed in this deployment.
Check System Grants Run Flag	Y	required	Flag to indicate whether the workflow should run the system grants check. Valid values are Y (run the check) or N (do not run the check).
Execute Rollback	no default	required	Flag to indicate whether an automatic rollback will be performed whenever an error is detected during the execution of the SQL scripts. If Y is specified and an error occurs, the workflow exits and rolls back all committed SQL transactions that belong to the deployed SQL scripts. If N is specified, no rollback will be performed in the event of an error.
Oracle OS User	no default	required	The user who owns ORACLE_HOME.
Oracle Password	no default	required	Password for the Oracle Database user.
Oracle User	no default	required	Oracle Database user who will execute the SQL scripts.
Rollback File	no default	required if Execute Rollback is enabled	The file name and path of the rollback script file that records all SQL transactions performed by the SQL scripts. This file can be used to: <ul style="list-style-type: none"> Perform an automatic rollback in the event of an error Execute a rollback at a later time

Input Parameters for Gather Parameters for Oracle SQL Release, continued

Parameter Name	Default Value	Required	Description
			<ul style="list-style-type: none"> ○ Serve as an audit file for future use
SQL Scripts	script.sql	required	<p>Comma-separated list of SQL script files that will be deployed to the target servers. These files will be downloaded from the software repository if they do not already exist on the target server. SQL script files can have arguments. For example:</p> <p>MySQLfile1.sql arg1, MySQLfile2.sql arg2 arg3, MySQLfile3.sql</p> <p>Note: List the SQL script files in the order in which they need to be executed.</p>
Staging Directory	/tmp/	optional	The directory on the target server where the SQL script file (or files) will be downloaded.

Tip: To avoid having to re-enter passwords whenever they change, you can create a policy to provide them to the workflow.

Note: See ["Parameters for Oracle - SQL Release v3" on page 566](#) for detailed descriptions of all input parameters for this workflow, including default values.

3. In the workflow editor, expose any additional parameters that you need. You will specify values for those parameters when you create the deployment.
4. Save the changes to the workflow (click **Save** in the lower right corner).
5. Create a new deployment.
6. On the Parameters tab, specify values for the required parameters listed in step 2 and any additional parameters that you have exposed. You do not need to specify values for those parameters whose default values are appropriate for your environment.
7. On the Targets tab, specify one or more targets for this deployment.
8. Save the deployment (click **Save** in the lower right corner).
9. Run the workflow using this deployment.

To verify the results:

The workflow will complete and report SUCCESS on the Console if it has run successfully. If an error occurs during workflow execution, the error is logged, and the workflow terminates in the FAILURE state.

Optional: If you want to further verify the results:

Log in to your database to make sure that whatever you created or modified was actually done.

Sample Scenarios

This topic shows you typical parameter values for different use cases for the "Oracle - SQL Release v3" workflow.

Scenario 1: Deploy and execute the scripts

This is a very simple example that you might use in a development environment. None of the optional checks of the SQL scripts are performed. SQL syntax errors will be ignored. The workflow will create an SQL*Plus session to deploy and execute the scripts. It will not save a rollback file. It will not perform an automatic rollback if an error is encountered when executing the SQL scripts.

Archive logging can be off since Execute Rollback is not enabled.

Parameters Defined in this Step: Gather Parameters for Oracle SQL Release

Parameter Name	Example	Description
Check Database Links Run Flag	N	Flag to indicate whether the workflow should run the database links check. Valid values are Y (run the check) or N (do not run the check).
Check Prohibited Statements Run Flag	N	Flag to indicate whether the workflow should run the prohibited statements check. Valid values are Y (run the check) or N (do not run the check).
Check SQL Syntax Database Type	dbvoracle	Database type used to set the SQL parser. For example: dbvoracle, dbvsybase, dbvmssql, or dbvdb2. See SQL Parser Documentation for valid options.
Check SQL Syntax Ignore Errors	True	Flag to indicate whether the workflow should pass the SQL syntax check regardless of whether or not syntax errors are found. Valid values are True (the check will always pass) or False (the check will fail if syntax errors are present).
Check System Grants Run Flag	N	Flag to indicate whether the workflow should run the system grants check. Valid values are Y (run the check) or N (do not run the check).
Execute Rollback	N	Flag to indicate whether an automatic rollback will be performed whenever an error is detected during the execution of the SQL scripts. If Y is specified and an error occurs, the workflow exits and rolls back all committed SQL transactions that belong to the deployed SQL scripts. If N is specified, no rollback will be performed in the event of an error.
Oracle OS User	oracle	The user who owns ORACLE_HOME.
Oracle Password	tiger	Password for the Oracle Database user.
Oracle	scott	Oracle Database user who will execute the SQL scripts.

Parameters Defined in this Step: Gather Parameters for Oracle SQL Release, continued

Parameter Name	Example	Description
User		
SQL Scripts	see description	<p>Comma-separated list of SQL script files that will be deployed to the target servers. These files will be downloaded from the software repository if they do not already exist on the target server. SQL script files can have arguments. For example:</p> <pre>MySQLfile1.sql arg1, MySQLfile2.sql arg2 arg3, MySQLfile3.sql</pre> <p>Note: List the SQL script files in the order in which they need to be executed.</p>
SQL Script Output	True	The output of SQL script execution will be displayed on DMA console.

Scenario 2: Check the SQL script files, deploy and execute the scripts, then perform a rollback if an error is encountered

This is a more complex example that you might use in a production environment where you desire more safeguards.

Archive logging must be enabled for this use case.

The workflow will check the SQL script files for:

- Oracle database links
- The Oracle system grants that are specified in the Exception List parameter
- The regular expression that is specified in the Regular Expression parameter
- SQL syntax errors

If no errors were found in the checks, the workflow creates an SQL*Plus session to deploy and execute the scripts. It will save a rollback file and perform an automatic rollback if an error is encountered when executing the SQL scripts.

Parameters Defined in this Step: Gather Parameters for Oracle SQL Release

Parameter Name	Example	Description
Acceptable ORA Error	ORA-00942	Comma-separated list of ORA errors that will be expected (and can be ignored) while running release scripts. For example: ORA-00942
Check Database Links Run Flag	Y	Flag to indicate whether the workflow should run the database links check. Valid values are Y (run the check) or N (do not run the check).
Check Prohibited Statements Regular Expression	drop\s+table	The regular expression to be searched for in all of the SQL scripts to be deployed. If the specified regular expression is found, the workflow exits with a failure. For example: drop\s+table will match all statements that drop a table.
Check Prohibited Statements Run Flag	Y	Flag to indicate whether the workflow should run the prohibited statements check. Valid values are Y (run the check) or N (do not run the check).
Check SQL Syntax Database Type	dbvoracle	Database type used to set the SQL parser. For example: dbvoracle, dbvsybase, dbvmssql, or dbvdb2. See SQL Parser Documentation for valid options.
Check SQL Syntax Ignore Errors	False	Flag to indicate whether the workflow should pass the SQL syntax check regardless of whether or not syntax errors are found. Valid values are True (the check will always pass) or False (the check will fail if syntax errors are present).

Parameters Defined in this Step: Gather Parameters for Oracle SQL Release, continued

Parameter Name	Example	Description
Check System Grants Exception List	CREATE VIEW, CREATE SYNONYM, CREATE CLUSTER, CREATE TABLE	Comma-separated list of system privileges that are not allowed in this deployment.
Check System Grants Run Flag	Y	Flag to indicate whether the workflow should run the system grants check. Valid values are Y (run the check) or N (do not run the check).
Execute Rollback	Y	Flag to indicate whether an automatic rollback will be performed whenever an error is detected during the execution of the SQL scripts. If Y is specified and an error occurs, the workflow exits and rolls back all committed SQL transactions that belong to the deployed SQL scripts. If N is specified, no rollback will be performed in the event of an error.
Oracle OS User	oracle	The user who owns ORACLE_HOME.
Oracle Password	tiger	Password for the Oracle Database user.
Oracle User	scott	Oracle Database user who will execute the SQL scripts.
Rollback File	/var/tmp/ rollback.sql	The file name and path of the rollback script file that records all SQL transactions performed by the SQL scripts. This file can be used to: <ul style="list-style-type: none"> • Perform an automatic rollback in the event of an error • Execute a rollback at a later time • Serve as an audit file for future use
SQL Scripts	see description	Comma-separated list of SQL script files that will be deployed to the target servers. These files will be downloaded from the software repository if they do not already exist on the target server. SQL script files can have arguments. For example: MySQLfile1.sql arg1, MySQLfile2.sql arg2 arg3, MySQLfile3.sql Note: List the SQL script files in the order in which they need to be executed.

Be sure that the default values for all remaining input parameters are appropriate for your environment (see ["Parameters for Oracle - SQL Release v3" on the next page](#)).

Parameters for Oracle - SQL Release v3

The following tables describe the required and optional input parameters for this workflow. Some of these parameters may not be initially visible in a deployment. For some parameters, if you do not specify a value for a parameter, a default value is assigned.

Note: Only those parameters that are configurable in a standard deployment are listed here. Input parameters that must be mapped to output parameters of previous steps are not listed.

Input Parameters Defined in this Step: Gather Parameters for Oracle SQL Release

Parameter Name	Default Value	Required	Description
Acceptable ORA Error		optional	Comma-separated list of ORA errors that will be expected (and can be ignored) while running release scripts. For example: ORA-00942
Check Database Links Run Flag	Y	required	Flag to indicate whether the workflow should run the database links check. Valid values are Y (run the check) or N (do not run the check).
Check Prohibited Statements Regular Expression		optional	The regular expression to be searched for in all of the SQL scripts to be deployed. If the specified regular expression is found, the workflow exits with a failure. For example: drop\s+table will match all statements that drop a table.
Check Prohibited Statements Run Flag	no default	required	Flag to indicate whether the workflow should run the prohibited statements check. Valid values are Y (run the check) or N (do not run the check).
Check SQL Syntax Database Type	dbvoracle	optional	Database type used to set the SQL parser. For example: dbvoracle, dbvsybase, dbvmssql, or dbvdb2. See SQL Parser Documentation for valid options.
Check SQL Syntax Ignore Errors	False	optional	Flag to indicate whether the workflow should pass the SQL syntax check regardless of whether or not syntax errors are found. Valid values are True (the check will always pass) or False (the check will fail if syntax errors are present).
Check System Grants Exception List	CREATE VIEW, CREATE SYNONYM, CREATE CLUSTER, CREATE TABLE	optional	Comma-separated list of system privileges that are not allowed in this deployment.
Check System Grants Run	Y	required	Flag to indicate whether the workflow should run the system grants check. Valid values are Y (run the check) or N (do not run the check).

Input Parameters Defined in this Step: Gather Parameters for Oracle SQL Release, continued

Parameter Name	Default Value	Required	Description
Flag			
Execute Rollback	no default	required	Flag to indicate whether an automatic rollback will be performed whenever an error is detected during the execution of the SQL scripts. If Y is specified and an error occurs, the workflow exits and rolls back all committed SQL transactions that belong to the deployed SQL scripts. If N is specified, no rollback will be performed in the event of an error.
Oracle OS User	no default	required	The user who owns ORACLE_HOME.
Oracle Password	no default	required	Password for the Oracle Database user.
Oracle User	no default	required	Oracle Database user who will execute the SQL scripts.
Rollback File	no default	required if Execute Rollback is enabled	The file name and path of the rollback script file that records all SQL transactions performed by the SQL scripts. This file can be used to: <ul style="list-style-type: none"> • Perform an automatic rollback in the event of an error • Execute a rollback at a later time • Serve as an audit file for future use
SQL Script Output	False	optional	If True, enables to view the output of SQL script execution on DMA console.
SQL Scripts	script.sql	required	Comma-separated list of SQL script files that will be deployed to the target servers. These files will be downloaded from the software repository if they do not already exist on the target server. SQL script files can have arguments. For example: MySQLfile1.sql arg1, MySQLfile2.sql arg2 arg3, MySQLfile3.sql Note: List the SQL script files in the order in which they need to be executed.
Staging Directory	/tmp/	optional	The directory on the target server where the SQL script file (or files) will be downloaded.

Microsoft SQL Server

Workflow type	Workflow name
Compliance	"MS SQL - Compliance Audit v2" on the next page
Provisioning	"MS SQL - Install Clustered SQL Instance v2" on page 674
	"MS SQL - Add Node to Cluster v3" on page 689
	"MS SQL - Create Database v2" on page 698
	MS SQL - Install Standalone SQL Instance
	"MS SQL - Upgrade Standalone SQL Instance" on page 653
	"MS SQL - Create AlwaysOn Availability Group v2" on page 667
Patching	"MS SQL - Install Patch" on page 583
	"MS SQL - Install Cluster Patch" on page 587
	"MS SQL Rollback Patch" on page 660
Refreshing	"MS SQL - Backup Database" on page 592
	"MS SQL - Backup and Restore Database" on page 615
	"MS SQL - Restore Database" on page 602
Release Management	"DB Release for SQL Server v2" on page 631

MS SQL - Compliance Audit v2

The MS SQL - Compliance Audit workflow enables you to audit a Microsoft SQL Server instance for compliance with the following security benchmark requirements:

- Center for Internet Security (CIS) security configuration benchmarks
- Payment Card Industry (PCI) data security standard
- Sarbanes-Oxley (SOX) requirements

The workflow performs CIS Level 1 and Level 2 auditing for a SQL Server instance. The audit identifies compliance related problems with a SQL Server instance.

The workflow performs the checks included in the CIS benchmark and then maps those CIS checks to the benchmark type that you specify in the Compliance Type parameter. The audit summary email will match the Compliance Type that you specify.

To use this workflow in your environment, see the following information:

Topic	Information Included
"Prerequisites for this Workflow"	List of prerequisites that must be satisfied before you can run this workflow
"How this Workflow Works"	Information about what the workflow does, including validation checks performed, steps executed, and step descriptions
"How to Run this Workflow"	Instructions for running this workflow in your environment
"Sample Scenarios"	Examples of typical parameter values for this workflow
Parameters	List of input parameters for this workflow

Prerequisites for this Workflow

Be sure that the following prerequisites are satisfied before you run the MS SQL - Compliance Audit v2 workflow:

- The latest DMA solution packs require the latest DMA platform. To use the latest solution packs, update the DMA platform. DMA10.50.001.000 solution packs are supported on DMA10.50.001.000 (and later).
- You have installed the Database Compliance solution pack.

The workflow must be able to:

- Execute `reg.exe` (Windows Server command-line registry tool), `wmic.exe` (Windows Management Instrumentation Command-line tool), and “net” Windows utilities on the target server. These utilities are included in the base Windows Server installations.
- Log in to the SQL Server instance using Windows-authenticated login credentials.
- Read system tables and execute system procedures upon connecting to the SQL Server instance.

For more information about prerequisites for Microsoft SQL Server, refer to the [Microsoft SQL Server Documentation](#).

How this Workflow Works

This workflow performs the following actions:

- Prepares to run the workflow by gathering information about the target SQLServerInstance and validating parameter values.
- Audits the various configuration settings specified in the pertinent CIS, SOX, or PCI benchmark.
- Composes and sends an email containing the results of the audit.

Note: The emails are sent through the mail server configured on the DMA server. You can configure the mail server in the path below:

DMA setup > Configuration > Outgoing Mail > Server.

Validation Checks Performed

This workflow validates the following conditions:

1. Either `sqlcmd.exe` or `osql.exe` must be installed on the target machine.
2. Any Excluded Checks specified by the user refer to actual CIS, SOX, or PCI benchmark checks.
3. Any email addresses specified are valid addresses.
4. The workflow can create the temporary file that will store the compliance check results.

Steps Executed

The MS SQL - Compliance Audit workflow includes the following steps. Each step must complete successfully before the next step can start. If a step fails, the workflow reports a failure and all subsequent steps are skipped.

Steps Used by Run MS SQL Compliance Audit

Workflow Step	Description
MS SQL - Gather Parameters for MS SQL Compliance	This step gathers two pieces of information: (1) the type of compliance audit to perform and (2) the list of compliance checks to exclude from the audit.
MS SQL - Gather Advanced Parameters for MS SQL Compliance	This step gathers the information that the workflow needs to create and deliver the compliance audit report via email. It also enables you to specify the name of the latest available SQL Server build and the Windows domain user.
Validate Compliance	This step validates the input parameters specified in the previous steps. It validates the list of excluded checks to ensure that all specified checks in the list

Steps Used by Run MS SQL Compliance Audit, continued

Workflow Step	Description
Parameters v2	<p>correspond to actual Center for Internet Security (CIS) benchmark items. It also validates the email information to ensure that all specified email addresses are valid.</p> <p>The step then creates the path to the temporary file that will store the results of the current audit as the workflow is running. This file is deleted after the audit report is sent.</p>
MS SQL-Prepare SQL Server Compliance Check	<p>This step determines whether workflow can perform the following actions on the target system:</p> <ul style="list-style-type: none"> • Check database connectivity • Query the registry • Check the registry for SQL Server • Execute Windows Management Instrumentation (WMI) API calls • Execute the <code>net user /?</code> command <p>If the workflow can perform all of these actions, it is capable of running the Center for Internet Security (CIS) Security Configuration Benchmark compliance tests.</p>
MS SQL - Compliance Checks	<p>This step executes all the compliance checks for MS SQL server.</p>
Validate Post Compliance Checks	<p>This step reads the temporary file that contains the results of the compliance audit and prints the audit results to the DMA Console. It also creates (or updates) the compliance metadata fields for the target.</p> <p>If email addresses were specified, it also creates a report in HTML format that will be emailed to those addresses by a later step in the workflow.</p>
Send Compliance Email v2	<p>If email addresses are provided, this step sends the previously generated compliance audit report to the specified email addresses.</p>
Delete File	<p>This step deletes the specified file on the target server.</p>

Note: For input parameter descriptions and defaults, see "[Parameters for MS SQL - Compliance Audit v2](#)" on page 582.

How to Run this Workflow

The following instructions show you how to customize and run the MS SQL - Compliance Audit v2 workflow in your environment.

The workflow provides default values for some parameters. These default values are usually sufficient for a "typical" installation. You can override the defaults by specifying parameter values in the deployment. You can also expose additional parameters in the workflow, if necessary, to accomplish more advanced scenarios. Any parameters not explicitly specified in the deployment will have the default values listed in ["Parameters for MS SQL - Compliance Audit v2" on page 582](#).

Note: Before following this procedure, review the ["Prerequisites for this Workflow" on page 570](#), and ensure that all requirements are satisfied.

To use the MS SQL Compliance Audit v2 workflow:

1. Create a deployable copy of the workflow.
2. Determine the values that you will specify for the following parameters:

Parameters Defined in this Step: Gather Parameters for SQL Server Compliance

Parameter Name	Default Value	Required	Description
Compliance Type	CIS	optional	Type of compliance report that will be generated by the workflow. Supported types are: CIS = Center for Internet Security (CIS) Security Configuration Benchmark PCI = Payment Card Industry (PCI) Data Security Standard SOX = Sarbanes-Oxley (SOX) sections 302.2, 302.4b, 302.4c, and 302.5 requirements
Excluded Checks	no default	optional	Comma-separated list of compliance checks to exclude from the audit. For example: 1.2, 2, 3.*, 5*, 6.1.2 Note: Make sure that the checks specified here correspond with the compliance audit type (CIS, PCI, or SOX) that you are running.

Parameters Defined in this Step: Advanced Parameter for MS SQL Compliance

Parameter Name	Default Value	Required	Description
Email Addresses to Receive Report	no default	optional	Comma-separated list of email addresses for those individuals or groups who will receive a copy of the compliance audit report.
Instance Account	no default	optional	The Windows account that will perform the compliance audit.
Instance Password	no default	optional	The password for the Windows account that will perform the compliance audit.
Latest Build to Check for	no default	optional	The latest build of SQL server according to Microsoft. For example, build 4439 for SQL Server 2014 SP1.

Note: This is the minimum set of parameters required to run this workflow. You may need to expose additional parameters depending on your objectives.

See ["Parameters for MS SQL - Compliance Audit v2" on page 582](#) for detailed descriptions of all input parameters for this workflow, including default values.

3. In the workflow editor, expose any additional parameters that you need. You will specify values for those parameters when you create the deployment or at runtime.
4. Save the changes to the workflow (click **Save** in the lower right corner).
5. Create a new deployment.
6. On the Parameters tab, specify values (or set the type to Runtime Value) for the required parameters listed in step 2 and any additional parameters that you have exposed. You do not need to specify values for those parameters whose default values are appropriate for your environment.
7. On the Targets tab, specify one or more targets for this deployment.
8. Save the deployment (click **Save** in the lower right corner).
9. Run the workflow using this deployment, specifying any runtime parameters.

To verify the results:

The workflow will complete and report SUCCESS on the Console if it has run successfully. If an error occurs during workflow execution, the error is logged, and the workflow terminates in the FAILURE state.

Information about each compliance check is displayed in the step output on the Console (and the History page) for each of the audit steps.

A summary of the compliance audit is also displayed in the step output for the Validate Post Compliance Checks step.

To view the reports:

A compliance audit summary in HTML format is emailed to all parties on the Email Addresses to Receive Report list.

After you run this workflow, you can generate two types of compliance reports on the Reports page:

- Database Compliance Report
- Database Compliance Detail Report

To access the Database Compliance reports:

1. Go to the Reports page.
2. At the bottom of the page, specify the following settings:

For the Database Compliance Report:

- a. Select the Database Compliance report.
- b. Select the organization where your target resides.
- c. Because this report lists the latest compliance audit reports for all targets in the specified organization, you do not specify a Server, Database, or Time span.

For the Database Compliance Detail Report:

- a. Select the Database Compliance Details report.
- b. Select the organization where your target resides.
- c. Specify the Server and Instance that you selected when you created your deployment.

3. Click **Run report**.

Sample Scenarios

This topic shows you how to use various parameters to achieve the following compliance audit scenarios in your environment using the "MS SQL - Compliance Audit v2" workflow.

Scenario 1: Perform a Partial CIS Compliance Audit and Email the Results

In the scenario, the following checks are excluded from the audit:

- Section 7: Replication
- Section 9: Surface Area Configuration Tool

A summary report is sent to the three parties listed in the Email Addresses to Receive Report parameter.

Parameter Name	Example Value	Description
Compliance Type	CIS	Type of compliance report that will be generated by the workflow. Supported types are: CIS = Center for Internet Security (CIS) Security Configuration Benchmark PCI = Payment Card Industry (PCI) Data Security Standard SOX = Sarbanes-Oxley (SOX) sections 302.2, 302.4b, 302.4c, and 302.5 requirements
Excluded Compliance Checks	7.*,9.*	Comma-separated list of compliance checks to exclude from the audit. For example: 1.2, 2, 3.*, 5*, 6.1.2 Note: Make sure that the checks specified here correspond with the compliance audit type (CIS, PCI, or SOX) that you are running.
Email Addresses to Receive Report	SQLDBAdminTeam@mycompany.com, SQLDBAdminMgr@mycompany.com, CustomerSupportTeam@mycompany.com	Comma-separated list of email addresses for those individuals or groups who

Parameter Name	Example Value	Description
		will receive a copy of the compliance audit report.

Note: Some of these parameters are not exposed by default in the deployment.

Be sure that the default values for all remaining input parameters are appropriate for your environment (see "[Parameters for MS SQL - Compliance Audit v2](#)").

Scenario 2: Perform a Full PCI Compliance Audit and Email the Results

A summary report is sent to the three parties listed in the Email Addresses to Receive Report parameter.

Parameter Name	Example Value	Description
Compliance Type	PCI	<p>Type of compliance report that will be generated by the workflow. Supported types are:</p> <p>CIS = Center for Internet Security (CIS) Security Configuration Benchmark</p> <p>PCI = Payment Card Industry (PCI) Data Security Standard</p> <p>SOX = Sarbanes-Oxley (SOX) sections 302.2, 302.4b, 302.4c, and 302.5 requirements</p>
Email Addresses to Receive Report	SQLDBAdminTeam@mycompany.com, SQLDBAdminMgr@mycompany.com, CustomerSupportTeam@mycompany.com	Comma-separated list of email addresses for those individuals or groups who will receive a copy of the compliance audit report.

Note: Some of these parameters are not exposed by default in the deployment.

Be sure that the default values for all remaining input parameters are appropriate for your environment (see "[Parameters for MS SQL - Compliance Audit v2](#)").

Scenario 3: Perform a Full SOX Compliance Audit, Email the Results, and Configure Windows Domain User Using Runtime Parameters

A summary report is sent to the three parties listed in the Email Addresses to Receive Report parameter.

Note: You may want to run this workflow against a MS SQL instance that can only be accessed by a Windows user with a temporary password. By using a runtime parameter for the password, you can ensure that the password used is always the latest.

To specify the Windows domain user at the time you execute a deployment with runtime parameters, perform the following additional steps:

1. When you make a copy of the workflow, expand the appropriate step, and then set the Windows domain user parameters—Instance Account and Instance Password—to **- User selected -**.
2. When you create a deployment from the copy of the workflow, set the parameter types to **Runtime Value**.
3. When you execute the deployment, specify the Windows domain user account and password.

Parameter Name	Example Value	Description
Compliance Type	SOX	Type of compliance report that will be generated by the workflow. Supported types are: CIS = Center for Internet Security (CIS) Security Configuration Benchmark PCI = Payment Card Industry (PCI) Data Security Standard SOX = Sarbanes-Oxley (SOX) sections 302.2, 302.4b, 302.4c, and 302.5 requirements
Email Addresses to Receive Report	SQLDBAdminTeam@mycompany.com, SQLDBAdminMgr@mycompany.com, CustomerSupportTeam@mycompany.com	Comma-separated list of email addresses for those individuals or groups who will receive a copy of the compliance audit report.
Instance Account	Domain\DomainUserAcct	The Windows account that will perform the compliance audit.

Parameter Name	Example Value	Description
	Note: Enter at runtime.	
Instance Password	DomainUserPswd Note: Enter at runtime.	The password for the Windows account that will perform the compliance audit.
Latest Build to Check for	5058	The latest build of Microsoft SQL Server 2005, according to Microsoft. Ensure that instance is at least patched up to indicated build level. Example value would be "5058" for SQL 2012's SP2. If no value is given, the related Compliance check will be skipped.

Note: Some of these parameters are not exposed by default in the deployment.

Be sure that the default values for all remaining input parameters are appropriate for your environment (see ["Parameters for MS SQL - Compliance Audit v2"](#)).

Scenario 4: Perform a Full CIS Compliance Audit and Display the Results on the DMA Console

In the scenario, all scorable checks are performed, and the compliance audit report is displayed only on the DMA Console. In this case, a summary report is not emailed. This scenario would be appropriate for initial testing.

It is not necessary to specify any input parameters in this scenario unless the SQL Server inventory file is located in a non-standard directory.

Parameter Name	Example Value	Description
Compliance Type	CIS	Type of compliance report that will be generated by the workflow. Supported types are: CIS = Center for Internet Security (CIS) Security Configuration Benchmark PCI = Payment Card Industry (PCI) Data Security Standard SOX = Sarbanes-Oxley (SOX) sections 302.2, 302.4b, 302.4c, and 302.5 requirements

Be sure that the default values for all remaining input parameters are appropriate for your environment (see ["Parameters for MS SQL - Compliance Audit v2"](#)).

Parameters for MS SQL - Compliance Audit v2

The following tables describe the required and optional input parameters for this workflow. Some of these parameters are not initially visible in a deployment. For most parameters, if you do not specify a value for a parameter, a default value is assigned.

Only those parameters that are configurable in a standard deployment are listed here. Input parameters that must be mapped to output parameters of previous steps are not listed.

Parameters Defined in this Step: Gather Parameters for MS SQL Compliance

Parameter Name	Default Value	Required	Description
Compliance Type	CIS	optional	Type of compliance report that will be generated by the workflow. Supported types are: CIS = Center for Internet Security (CIS) Security Configuration Benchmark PCI = Payment Card Industry (PCI) Data Security Standard SOX = Sarbanes-Oxley (SOX) sections 302.2, 302.4b, 302.4c, and 302.5 requirements
Excluded Checks	no default	optional	Comma-separated list of compliance checks to exclude from the audit. For example: 1.2, 2, 3.*, 5*, 6.1.2 Note: Make sure that the checks specified here correspond with the compliance audit type (CIS, PCI, or SOX) that you are running.

Parameters Defined in this Step: Gather Advanced Parameters for MS SQL Compliance

Parameter Name	Default Value	Required	Description
Email Addresses to Receive Report	no default	optional	Comma-separated list of email addresses for those individuals or groups who will receive a copy of the compliance audit report.
Instance Account	no default	optional	The Windows account that will perform the compliance audit.
Instance Password	no default	optional	The password for the Windows account that will perform the compliance audit.
Latest Build to Check for	no default	optional	The latest build of Microsoft SQL Server 2005, according to Microsoft. Ensure that instance is at least patched up to indicated build level. Example value would be "5058" for SQL 2012's SP2. If no value is given, the related Compliance check will be skipped.

MS SQL - Install Patch

This section describes how to use Database and Middleware Automation (DMA) to create a repeatable, standardized method to quickly and accurately install Microsoft Microsoft SQL Server patches on SQL Server installations across an enterprise to reach patch currency standards.

Tip: To patch more complex SQL Server clustered environments, see *Achieve Patch Currency for Microsoft SQL Server Clustered Environments Using DMA*, available at:
<https://softwaresupport.hp.com/>

Prerequisites

Before performing the procedures in this section, your environment must meet the following minimum requirements:

- A server running Windows 2008, 2008 R2, or 2012.
- A SQL Server instance—version 2005, 2008, 2008R2, or 2012—is provisioned and ready to be patched.
- Patch media:

The SQL Server patch file from Microsoft.

Patch installation media must be available locally or available for download from the software repository.

- Storage: A staging directory with 1 gigabyte available.
- Licenses for SQL Server and DMA.

Process Overview

Installing a SQL Server patch to a Microsoft SQL Server installation with DMA is a simple, one-step process. All required checks and steps have been implemented in a single DMA workflow.

Use the following DMA workflow to standardize the process of installing a SQL Server patch:

DMA can install any of the following types of SQL Server patches:

- Hot Fixes
- Cumulative Updates
- Service Packs

Note: This workflow patches a single SQL Server instance unless you use the advanced parameter Patch All Instances on Server. The advanced parameter is demonstrated in this section.

Tip: To patch multiple SQL Server cluster nodes, run MS SQL - Install Patch once for each node, or for an easier process, use the MS SQL - Install Cluster Patch workflow that is described in *Achieve Patch Currency for Microsoft SQL Server Clustered Environments Using DMA*, available at: <https://softwaresupport.hp.com/>

Workflow: MS SQL - Install Patch



This section provides detailed information required to run the MS SQL - Install Patch workflow.

Tip: To patch multiple SQL Server cluster nodes, run MS SQL - Install Patch once for each.

Solution pack

This workflow requires the Database Patching Solution Pack.

Parameters to expose

If you want to patch all SQL Server instances, in the workflow's MS SQL - Advanced Parameters - Install Patch step, expose the Patch All Instances on Server parameter.¹

Input parameters

When you deploy the MS SQL - Install Patch workflow, specify input parameter values for the following steps.

Bold text in the following tables indicates that you must specify a value for the parameter.

Step: MS SQL - Parameters - Install Patch

Parameter	Description	Example Value
Download From Software Directory	<p>Required: The name of the SQL Server patch file obtained from Microsoft.²</p> <p>Note: This must be an EXE file. If you obtain a ZIP file from Microsoft, unzip it to retrieve the EXE file.</p>	SQL12_SP1.exe
Download Target Destination	<p>Required: The local directory where the SQL Server patch file is stored:</p> <p>If patch file is in the software repository: Location where Download From Software Directory will be downloaded</p> <p>If patch file is on the target: Location where the Microsoft SQL Server patch file already exists</p> <p>Upon a successful workflow completion, all downloaded files are cleaned up.</p>	C:\temp
Web Service Password	Required: Password for the DMA Discovery web service API.	●●●
Web Service User	Required: User who is capable of modifying the managed environment by using the DMA Discovery web service API.	dmawebuser

¹This parameter is hidden by default and must be exposed when you make a copy of the workflow.

²If the file is not found on the target server(s), it will be downloaded from the software repository.

Step: MS SQL - Advanced Parameters - Install Patch

Parameter	Description	Example Value
Backup Path	Optional: Specifies the location for the backups of SQL Server databases. If left blank, the Instance default setting will be used.	?
Backup Type	Optional: backup type. Valid values are FULL, LOG, DIFFERENTIAL, COPY-ONLY, COPY-ONLY LOG. If none is provided, FULL backup will be taken.	FULL
Cluster Administrator Account	Required for patches on clustered instances: The domain user that will run the setup operation. This user requires elevated administrator privileges on the cluster. Acceptable format: [DOMAIN]\[USERNAME]	Win12\Administrator
Cluster Administrator Password	Required for patches on clustered instances: Password for the domain user that will run the setup operation. This user requires elevated administrator privileges on the cluster. Must be a strong Windows password.	●●●
Download From Software Directory	Optional: Downloads the software binaries.	?
Download Target Destination	Optional: Downloads the target destination.	?
Installer Account	Windows account that will be performing the install. Acceptable value is in format [DOMAIN]\[USERNAME]	Win12\Administrator
Installer Password	Password of Windows account that will be performing the install. Must be a strong Windows password.	●●●
Network Share File	Optional: Path to the patch file on a Windows network share. Path should begin with "\\<hostname>".	?
Patch All Instances on Server	Optional: Flag to determine whether all SQL Server instances on the server will be patched. Valid values: Yes or No. Default: No.	Yes

Step: MS SQL Kill Processes

Parameter	Description	Example Value
Instance Account	Optional: The Windows account that will terminate the SQL Server processes.	

FAQs

How do I install the SQL Server patch on all instances on the server?

To install the SQL Server patch on all instances on the server, set the Patch All Instances on Server parameter to Yes before you execute the deployment:

Workflow: MS SQL - Install Patch

Step: MS SQL - Advanced Parameters - Install Patch

Parameter: Patch All Instances on Server¹

How do I install the SQL Server patch on multiple cluster nodes?

To install the SQL Server patch on multiple cluster nodes, run the MS SQL - Install Patch workflow once on each cluster node.

MS SQL - Install Cluster Patch

This section describes how to use Database and Middleware Automation (DMA) to create a repeatable, standardized method to quickly and accurately install Microsoft SQL Server patches on SQL Server clustered installations across an enterprise to reach patch currency standards.

Tip: To patch SQL Server standalone environments, see *Achieve Patch Currency for Microsoft SQL Server Environments Using DMA*, available at: [softwaresupport.hp.com](https://software.support.hp.com)

¹This parameter is hidden by default and must be exposed when you make a copy of the workflow.

Prerequisites

Before performing the procedures in this section, your environment must meet the following minimum requirements:

- A server running Windows 2008, 2008 R2, or 2012.
- A SQL Server clustered instance—version 2008, 2008 R2, or 2012—is provisioned and ready to be patched.
- Patch media:

The SQL Server patch file from Microsoft.

Patch installation media must be available locally or available for download from the software repository.

- Storage: A staging directory with 1 gigabyte available.
- Licenses for SQL Server and DMA.

Process Overview

Installing a SQL Server patch to a Microsoft SQL Server clustered installation with DMA is a simple, one-step process. All required checks and steps have been implemented in a single DMA workflow.

DMA can install any of the following types of SQL Server patches:

- Hot Fixes
- Cumulative Updates
- Service Packs

Note: To execute the workflow, only one of the nodes in the SQL Server cluster needs to be a target for the deployment. The workflow discovers all cluster members and patches each one.

The following section provides detailed information required to run the workflow.

Workflow: MS SQL - Install Cluster Patch



This section provides detailed information required to run the MS SQL - Install Cluster Patch workflow.

Solution pack

This workflow requires the Database Patching Solution Pack.

Parameters to expose

None

Input parameters

When you deploy the MS SQL - Install Cluster Patch workflow, specify input parameter values for the following steps.

Step: MS SQL - Parameters - Install Patch

Parameter	Description	Example Value
Download From Software Directory	Required: The name of the SQL server patch file obtained from Microsoft. ¹ Note: This must be an EXE file. If you obtain a ZIP file from Microsoft, unzip it to retrieve the EXE file.	SQL12_SP1.exe
Download Target Destination	Required: The local directory where the SQL server patch file is stored: If patch file is in the software	C:\temp

¹ If the file is not found on the target server(s), it will be downloaded from the software repository.

Step: MS SQL - Parameters - Install Patch, continued

Parameter	Description	Example Value
	<p>repository: Location where Download From Software Directory will be downloaded</p> <p>If patch file is on the target: Location where the Microsoft SQL server patch file already exists</p> <p>Upon a successful workflow completion, all downloaded files are cleaned up.</p>	
Web Service Password	Required: Password for the DMA Discovery web service API.	●●●

Note: The step Run Subflow - MS SQL - Install Patch runs first to patch all passive nodes.

Step: Run Subflow - MS SQL - Install Patch

Parameter	Description	Example Value
Server Parallel Execution	Optional: Flag to determine whether the workflow is to execute in parallel. Set to False if you would like the workflow to execute serially. Default is True.	True

Note: The step Run Subflow - MS SQL - Install Patch runs again to patch the active node.

Step: Run Subflow - MS SQL - Install Patch

Parameter	Description	Example Value
Server Parallel Execution	Optional: Flag to determine whether the workflow is to execute in parallel. Set to False if you would like the workflow to execute serially. Default is True.	True

FAQs

How do I install the SQL Server patch on all instances on the server?

To install the SQL Server patch on all instances on the server, set the Patch All Instances on Server parameter to Yes before you execute the deployment:

Workflow: MS SQL - Install Patch

Step: MS SQL - Advanced Parameters - Install Patch

Parameter: Patch All Instances on Server¹

How do I install the SQL Server patch on multiple cluster nodes?

To install the SQL Server patch on multiple cluster nodes, run the MS SQL - Install Patch workflow once on each cluster node.

Refreshing Database

This section describes the SQL Server workflows included in the Database and Middleware Automation (DMA) Database Refresh solution pack.

Database refresh involves copying the contents of one database into a database in the same or another SQL Server instance. This is useful, for example, if you want to move a database from a traditional IT infrastructure to a private cloud. It is also useful if you want to duplicate production data in a test environment for application development or troubleshooting purposes.

The workflows in this solution pack enable you to automate and simplify the following operations:

- Extracting the contents of a database into a backup file
- Restoring a database from an existing backup file
- Extracting the contents of one database and loading them into another database using a single **bridged execution** workflow that performs both steps

The workflows perform extensive validation checks prior to and immediately after the database backup and restore operations to ensure that the refresh is successful.

After a refresh is completed, the restore workflows can re-create any existing database users and roles.

The workflows can create or utilize a database backup file that is compressed, encrypted, or both.

¹This parameter is hidden by default and must be exposed when you make a copy of the workflow.

MS SQL - Backup Database

This workflow enables you to backup a SQL Server database into file (the backup file) that is stored either locally or on a network share.

You can specify various options for the backup operation, including whether the backup file is compressed or encrypted with a password.

The workflow performs extensive validation checks prior to and immediately after the backup operation to ensure that the backup file is valid. The workflow will perform an additional integrity check on the backup file if you set the Perform Integrity Check parameter to YES.

To use this workflow in your environment, see the following information:

Topic	Information Included
"Prerequisites for this Workflow"	List of prerequisites that must be satisfied before you can run this workflow
"How this Workflow Works"	Information about what the workflow does, including validation checks performed, steps executed, and a high-level process flow
"How to Run this Workflow"	Instructions for running this workflow in your environment
"Sample Scenarios"	Examples of typical parameter values for this workflow
"Parameters for Backup MS SQL Database"	List of input parameters for this workflow

The process of deploying and running this workflow is the same for all scenarios, but the parameters required will differ depending on the specific scenario that you are implementing.

The workflow provides default values for most parameters. These default values are usually sufficient for a "typical" database backup. You can override the defaults by specifying parameter values in the deployment. You can also expose additional parameters in the workflow, if necessary, to accomplish more advanced scenarios.

Any parameters not explicitly specified in the deployment will have the default values listed in ["Parameters for Backup MS SQL Database" on page 599](#).

Prerequisites for this Workflow

The following prerequisites must be satisfied before you can run the ["MS SQL - Backup Database"](#) workflow:

1. The service login for the SQL Server service must have read and write permissions on the backup path.
2. The server management agent must have login access to the SQL Server instance in which the target database resides. It must also have permission to perform database consistency check (DBCC) commands on the target database.
3. There must be sufficient space available on the target data and log disks. The workflow checks for this, and will fail if sufficient space is not available.

Additional Considerations

For information about prerequisites for SQL Server, refer to the [SQL Server Product Documentation](#).

How this Workflow Works

This topic contains information about the "MS SQL - Backup Database" workflow:

Validation Checks Performed

The workflow checks the following things prior to dumping the database. If any of these checks fails, the workflow fails.

1. All required parameters have values. If any required parameter does not have a value—either a value that you specify or a default value—the workflow fails in the Run MS SQL Pre-Backup Validation step.
2. The Target Backup Path is accessible, either locally or on a network share.

If the Target Backup Path is on a network share, the Windows Share User has read and write access the share.
3. The target database exists, and the workflow can connect to it.
4. Adequate disk space is available to store the database backup file.
5. If the Target Backup Path does not currently exist, it will be created prior to creating the backup file.

Steps Executed

The "MS SQL - Backup Database" workflow includes the following steps. Each step must complete successfully before the next step can start. If a step fails, the workflow reports a failure, and all subsequent steps are skipped.

Process Flow

This workflow performs the following tasks:

1. Performs the preliminary [validation checks](#) described above.
2. Performs the database backup operation to create the backup file.
3. Performs post-backup validation checks to ensure that all required parameters had valid values.
4. If Perform Integrity Check was set to YES, performs an integrity check on the backup file.

Tips and Best Practices

It is good practice to run basic database consistency checks (DBCCs) on the source database before running this workflow to ensure that there are no internal errors in the database.

If you find errors in the source database, be sure to fix them before running this workflow. The workflow does not have the ability to diagnose or remediate problems in the database prior to performing the database backup.

How to Run this Workflow

This topic explains how to customize and run the "MS SQL - Backup Database" workflow in your environment.

Note: Prior to running this workflow, review the "Prerequisites for this Workflow", and ensure that all requirements are satisfied.

To customize and run the Backup MS SQL Database workflow:

1. Create a deployable copy of the workflow.
2. Determine the values that you will specify for the following parameter. This is the minimum set of parameters required to run this workflow.

Parameter Name	Default Value	Description
Target Backup Path	no default	<p>Where the database backup file will be stored, either locally or on a network share. You can specify both the path and file name, or you can specify only the path.</p> <ul style="list-style-type: none"> ◦ If you specify a file name, it must end in .bak. ◦ If you do not specify a file name, the backup file name will have the following form: <pre><dataBaseName>_<dateTime>.bak</pre> <p>where <i><dataBaseName></i> represents the name of the target database specified when the workflow runs, and <i><dateTime></i> is the date and time when the Run MS SQL Pre-Backup Validation step is executed.</p> <p>If the file will be stored on a network share, the Windows Share User must have read and write access to that share.</p>

3. See "Parameters for Backup MS SQL Database" on page 599 for detailed descriptions of all input parameters for this workflow, including default values. In the workflow editor, expose any additional parameters that you need. You will specify values for those parameters when you create the deployment or at runtime.
4. Save the changes to the workflow (click **Save** in the lower right corner).
5. Create a new deployment.
6. On the Parameters tab, specify values (or set the type to Runtime Value) for the required parameters listed in step 2 and any additional parameters that you have exposed. You do not need to specify values for those parameters whose default values are appropriate for your environment.
7. On the Targets tab, specify one or more targets for this deployment.
8. Save the deployment (click **Save** in the lower right corner).
9. Run the workflow using this deployment, specifying any runtime parameters.

The workflow will complete and report “Success” on the Console if it has run successfully. If an invalid parameter value is specified, an error is logged, and the workflow terminates in the “Failure” state.

Sample Scenarios

This topic shows you how to use various parameters to achieve the following database backup scenarios in your environment using the ["MS SQL - Backup Database"](#) workflow:

Scenario 1: Create a Backup File that is Not Encrypted or Compressed

This is the simplest SQL Server database backup scenario. In this example, the backup file is stored on a network share.

Step Name	Parameter Name	Example Value
Gather Parameters for MS SQL Database Backup	Target Backup Path	\\WIN-DOMAIN-CTRL\Backups
Gather Advanced Parameters for MS SQL Database Backup	Windows Share Password	WinSharePwd To avoid having to re-enter passwords whenever they change, you can create a policy to provide them to the workflow.
	Windows Share User	WIN\Administrator

Be sure that the default values for all remaining parameters are appropriate for your environment (see ["Parameters for Backup MS SQL Database"](#) on page 599).

Scenario 2: Create a Backup File that is Encrypted and Compressed

This scenario requires you to specify the encryption password and compression option for the database backup file. In this example, the backup file is stored locally on the server that hosts the target database.

Step Name	Parameter Name	Example Value
Gather Parameters for MS SQL Database Backup	Target Backup Path	c:\Backups\mytestdb_03122012.bak
Gather Advanced Parameters for MS SQL Database Backup	Backup Encryption Password	EncryptMyBackup
	Compress Backup File	YES

Be sure that the default values for all remaining parameters are appropriate for your environment (see ["Parameters for Backup MS SQL Database"](#) on page 599).

Scenario 3: Create a Backup File, Perform an Integrity Check, and Configure Windows Domain User Using Runtime Parameters

This scenario runs an integrity check on the backup file after the backup is performed. In this example, the backup file is stored locally on the server that hosts the target database.

Note: You may want to run this workflow against a MS SQL instance that can only be accessed by a Windows user with a temporary password. By using a runtime parameter for the password, you can ensure that the password used is always the latest.

To specify the Windows domain user at the time you execute a deployment with runtime parameters, perform the following additional steps:

1. When you make a copy of the workflow, expand the appropriate step, and then set the Windows domain user parameters—Instance Account and Instance Password—to **- User selected -**.
2. When you create a deployment from the copy of the workflow, set the parameter types to **Runtime Value**.
3. When you execute the deployment, specify the Windows domain user account and password.

Step Name	Parameter Name	Example Value
Gather Parameters for MS SQL Database Backup	Target Backup Path	c:\Backups\mytestdb_03122012.bak
Gather Advanced Parameters for MS SQL Database Backup	Perform Integrity Check	YES
	Instance Account	Domain\DomainUserAcct Note: Enter at runtime.
	Instance Password	DomainUserPswd Note: Enter at runtime.

Be sure that the default values for all remaining parameters are appropriate for your environment (see ["Parameters for Backup MS SQL Database" on the next page](#)).

Parameters for Backup MS SQL Database

The following tables describe the required and optional input parameters for this workflow. Most of these parameters are not initially visible in a deployment. For most parameters, if you do not specify a value for a parameter, a default value is assigned

Parameters Defined in this Step: Gather Parameters for MS SQL Database Backup

Parameter Name	Default Value	Required	Description
Target Backup Path	no default	required	<p>Where the database backup file will be stored, either locally or on a network share. You can specify both the path and file name, or you can specify only the path.</p> <ul style="list-style-type: none"> If you specify a file name, it must end in .bak. If you do not specify a file name, the backup file name will have the following form: <code><dataBaseName>_<dateTime>.bak</code> where <code><dataBaseName></code> represents the name of the target database specified when the workflow runs, and <code><dateTime></code> is the date and time when the Run MS SQL Pre-Backup Validation step is executed. <p>If the file will be stored on a network share, the Windows Share User must have read and write access to that share.</p>

Additional Parameters Defined in this Step: Gather Advanced Parameters for MS SQL Database Backup

Parameter Name	Default Value	Required	Description
Backup Description	no default	optional	Text that describes this backup (up to 255 characters).
Backup Encryption Password	no default	optional	<p>To encrypt the backup file with a password, specify the password in this parameter.</p> <p>If you perform the backup using a password, you must also specify that password when you perform the restore.</p>
Backup Name	no default	optional	The name of this backup (up to 128 characters).
Compress Backup File	NO	optional	<p>If you specify YES, the backup file will be compressed. Valid values: YES or NO.</p> <p>Compression is supported on SQL Server 2008</p>

Additional Parameters Defined in this Step: Gather Advanced Parameters for MS SQL Database Backup, continued

Parameter Name	Default Value	Required	Description
			Enterprise and later. If you are running SQL 2005, and this parameter is set to YES, the workflow will ignore this value and continue without compression.
Expiration Date	no default	optional	<p>Date and time when the backup file expires and the backup data is no longer considered relevant. After this date and time, SQL Server is not prevented from overwriting this backup file.</p> <p>The Expiration Date must be specified in a format compatible with the configured system datetime format.</p> <p>If both the Retention Days and the Expiration Date parameters are specified, the Retention Days parameter takes precedence.</p>
Instance Account	no default	optional	The Windows account that will perform the backup operation.
Instance Password	no default	optional	The password for the Windows account that will perform the backup operation.
Perform Integrity Check	NO	optional	If you specify YES, the workflow will perform an integrity check on the database backup file. Valid values: YES or NO.
Retention Days	no default	optional	<p>Number of days after which the backup data is no longer considered relevant. After this number of days, SQL Server is not prevented from overwriting this backup file.</p> <p>If both the Retention Days and the Expiration Date parameters are specified,</p>

Additional Parameters Defined in this Step: Gather Advanced Parameters for MS SQL Database Backup, continued

Parameter Name	Default Value	Required	Description
			the Retention Days parameter takes precedence.
Windows Share Password	no default	optional	Password for the user specified in Windows Share User.
Windows Share User	no default	optional	Windows user who can access the specified Windows network share and who will own (and write) the backup file.

MS SQL - Restore Database

This workflow enables you to restore a SQL Server database from a previously created database backup file that is stored locally, on a network share, or in the software repository.

If the database does not exist in the target instance, the workflow will create it. If the database already exists, you can specify whether you want the workflow to overwrite its contents. You can also specify whether existing database users should be re-created after the restore operation—in which case, any users included in the backup file are ignored.

Note: The parameters required to activate these options are hidden by default.

This workflow also provides a "simulation mode" where the Run MS SQL Pre-Restore Validation step is executed, but the restore is not performed. This is useful for testing or troubleshooting your parameter values.

The workflow performs extensive validation checks prior to and immediately after the restore operation to ensure that both the backup file and the restored database are valid.

The process of deploying and running this workflow is the same for all scenarios, but the parameters required will differ depending on the specific scenario that you are implementing.

The workflow provides default values for most parameters. These default values are usually sufficient for a "typical" database refresh. You can override the defaults by specifying parameter values in the deployment. You can also expose additional parameters in the workflow, if necessary, to accomplish more advanced scenarios.

Topic	Information Included
"Prerequisites for this Workflow"	List of prerequisites that must be satisfied before you can run this workflow
"How this Workflow Works"	Information about what the workflow does, including validation checks performed, steps executed, and a high-level process flow
"How to Run this Workflow"	Instructions for running this workflow in your environment
"Sample Scenarios"	Examples of typical parameter values for this workflow
"Parameters for Restore MS SQL Database"	List of input parameters for this workflow

The process of deploying and running this workflow is the same for all scenarios, but the parameters required will differ depending on the specific scenario that you are implementing.

The workflow provides default values for most parameters. These default values are usually sufficient for a "typical" database restore. You can override the defaults by specifying parameter values in the

deployment. You can also expose additional parameters in the workflow, if necessary, to accomplish more advanced scenarios.

Any parameters not explicitly specified in the deployment will have the default values listed in ["Parameters for Restore MS SQL Database" on page 613](#) .

Prerequisites for this Workflow

The following prerequisites must be satisfied before you can run the ["MS SQL - Restore Database"](#) workflow:

1. The service login for the SQL Server service must have read and write permissions on the backup file.
2. The server management agent must have login access to the target SQL Server instance. It must also have permission to create a new database and perform database consistency check (DBCC) commands on the restored database.
3. There must be sufficient space available on the target data and log disks. The workflow checks for this, and will fail if sufficient space is not available.

Additional Considerations

For information about prerequisites for SQL Server, refer to the [SQL Server Product Documentation](#).

How this Workflow Works

This topic contains information about the ["MS SQL - Restore Database"](#) workflow:

Validation Checks Performed

The workflow checks the following things prior to dumping the database. If any of these checks fails, the workflow fails.

1. All required parameters have values. If any required parameter does not have a value—either a value that you specify or a default value—the workflow fails in the Run MS SQL Pre-Restore Validation step.
2. The specified backup file either exists in the Download Target Destination directory or can be downloaded from the software repository.
3. The backup file is compatible with the target instance.
4. If the Custom Database Name parameter is specified, this database name complies with SQL Server database naming conventions.
5. The Download Target Destination is accessible, either locally or on a network share.

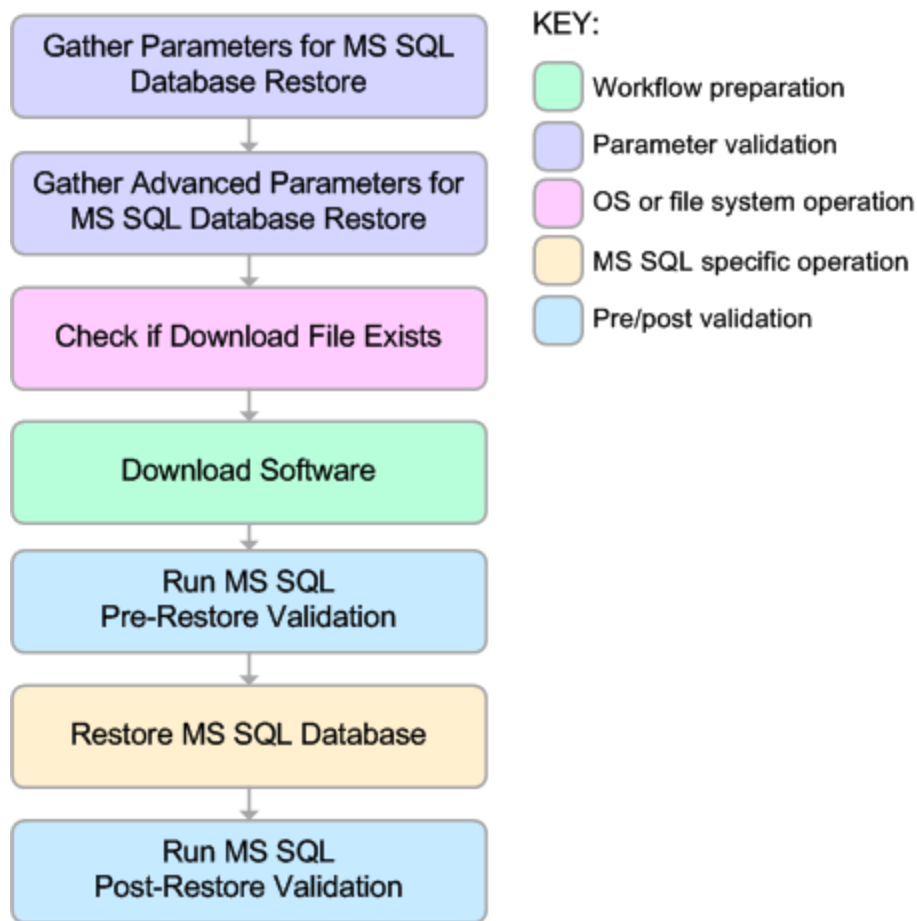
If the Download Target Destination is on a network share, the Windows Share User has read and write access to the share.

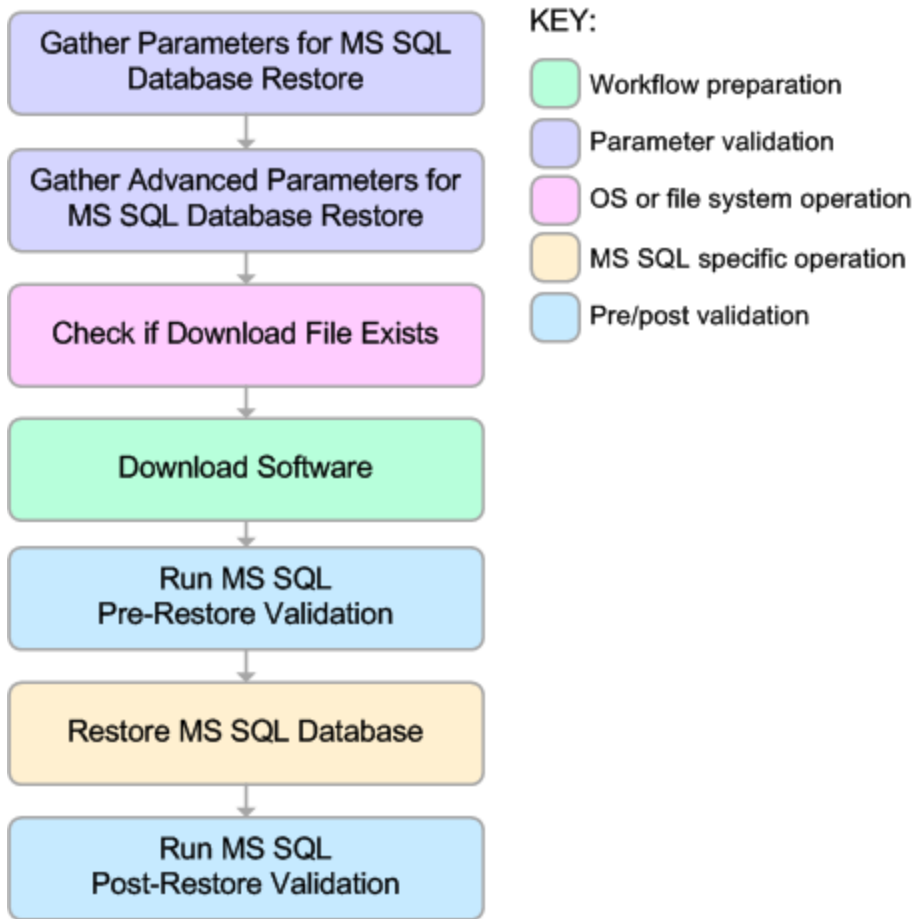
6. The target instance exists, and the workflow can connect to it.
7. Adequate disk space is available to restore the data and log files.
8. If custom paths are specified for the data or log files, the Run MS SQL Pre-Restore Validation step checks that they exist (and creates them if they don't), and ensures that the quantity of paths specified match the quantity of files in the backup file.

Steps Executed

The "MS SQL - Restore Database" workflow includes the following steps. Each step must complete successfully before the next step can start. If a step fails, the workflow reports a failure, and all subsequent steps are skipped.

Click each box in the diagram to view additional information about that step in a new window.





Process Flow

This workflow performs the following tasks:

1. Performs the preliminary **validation checks** described above.
2. If Preserve Users and Roles was set to YES, creates the Roles Creation Script and the Users Creation Script script.
3. If not in simulation mode, performs the database restore operation to load the contents of the backup file.
4. Performs post-restore validation checks to ensure that the restored database is sound.
5. If Preserve Users and Roles was set to YES, re-creates any existing database users and roles.
6. If Reindex Restored Database was set to YES, re-indexes the database.

Tips and Best Practices

It is good practice to run basic database consistency checks (DBCCs) on the source database before you create the database backup to ensure that there are no internal errors in the database.

If you find errors in the source database, be sure to fix them before you create the database backup. This workflow does not have the ability to diagnose or remediate problems in the database prior to performing the database backup.

How to Run this Workflow

This topic explains how to customize and run the ["MS SQL - Restore Database"](#) workflow in your environment.

Note: Prior to running this workflow, review the ["Prerequisites for this Workflow"](#), and ensure that all requirements are satisfied.

To customize and run the Restore MS SQL Database workflow:

1. Create a deployable copy of the workflow (see "Create a Deployable Workflow" in DMA Quick Start Tutorial).
2. Determine the values that you will specify for the following parameters. This is the minimum set of parameters required to run this workflow.

Parameter Name	Default Value	Description
Database Backup File	no default	<p>Path where the database backup file is (or will be) stored, either locally or on a network share.</p> <p>If the file already exists locally or on a network share, specify the file name in this parameter and the path in the Download Target Destination parameter.</p> <p>If the file does not yet exist locally or on a network share, it will be downloaded into this location from the software repository.</p> <p>If the file is (or will be) stored on a network share, the Windows Share User must have read and write access to that share.</p> <p>Note: Windows Share User and Windows Share Password are not exposed by default.</p>
Download Target Destination	no default	<p>The directory where the database backup file will be stored.</p> <p>If the database backup file does not yet exist in this directory, it will be downloaded from the software repository and stored in this directory.</p>

See ["Parameters for Restore MS SQL Database" on page 613](#) for detailed descriptions of all input parameters for this workflow, including default values.

3. In the workflow editor, expose any additional parameters that you need. You will specify values for those parameters when you create the deployment or at runtime.
4. Save the changes to the workflow (click **Save** in the lower right corner).
5. Create a new deployment.
6. On the Parameters tab, specify values (or set the type to Runtime Value) for the required parameters listed in step 2 and any additional parameters that you have exposed. You do not need

to specify values for those parameters whose default values are appropriate for your environment.

7. On the Targets tab, specify one or more targets for this deployment.
8. Save the deployment (click **Save** in the lower right corner).
9. Run the workflow using this deployment, specifying any runtime parameters.

The workflow will complete and report “Success” on the Console if it has run successfully. If an invalid parameter value is specified, an error is logged, and the workflow terminates in the “Failure” state.

Sample Scenarios

This topic shows you how to use various parameters to achieve the following database backup scenarios in your environment using the ["MS SQL - Restore Database"](#) workflow:

Scenario 1: Restore from a Backup File that is Not Encrypted or Compressed

This is the simplest SQL Server database restore scenario. In this example, the backup file has been stored on a network share (or will be downloaded from the software repository and stored on the share).

Note that the Windows Share User and Windows Share Password are specified in this scenario. This is not required, but it facilitates the disk space check on the network path. If you do not specify this parameter, this check is skipped.

Step Name	Parameter Name	Example Value
Gather Parameters for MS SQL Database Restore	Database Backup File	mytestdb_03122012.bak
	Download Target Destination	\\WIN-DOMAIN-CTRL\Backups
Gather Advanced Parameters for MS SQL Database Restore	Windows Share Password	WinSharePwd Tip: To avoid having to re-enter passwords whenever they change, you can create a policy to provide them to the workflow.
	Windows Share User	WIN\Administrator

Be sure that the default values for all remaining parameters are appropriate for your environment (see ["Parameters for Restore MS SQL Database"](#) on page 613).

Scenario 2: Restore from a Backup File that is Encrypted and Compressed

This scenario requires you to specify the encryption password for the database backup file. The workflow automatically handles the compression, so there is no need to specify the compression parameter. In this example, the backup file is stored locally on the server where the target instance resides.

Step Name	Parameter Name	Example Value
Gather Parameters for MS SQL Database Restore	Database Backup File	c:\Backups\mytestdb_03122012.bak
Gather Advanced Parameters for MS SQL Database Restore	Backup Encryption Password	EncryptMyBackup

Be sure that the default values for all remaining parameters are appropriate for your environment (see ["Parameters for Restore MS SQL Database"](#) on page 613).

Scenario 3: Overwrite an Existing Database, Restore Users, and Configure Windows Domain User Using Runtime Parameters

This scenario overwrites an existing database and restores any existing users after the restore is performed. In this example, the backup file is stored locally on the server where the target database resides.

Note: You may want to run this workflow against a MS SQL instance that can only be accessed by a Windows user with a temporary password. By using a runtime parameter for the password, you can ensure that the password used is always the latest.

To specify the Windows domain user at the time you execute a deployment with runtime parameters, perform the following additional steps:

1. When you make a copy of the workflow, expand the appropriate step, and then set the Windows domain user parameters—Instance Account and Instance Password—to **- User selected -**.
2. When you create a deployment from the copy of the workflow, set the parameter types to **Runtime Value**.
3. When you execute the deployment, specify the Windows domain user account and password.

Step Name	Parameter Name	Example Value
Gather Parameters for MS SQL Database Restore	Database Backup File	c:\Backups\mytestdb_03122012.bak
Gather Advanced Parameters for MS SQL Database Restore	Overwrite Existing Database	YES
	Preserve Users and Roles	YES
	Instance Account	Domain\DomainUserAcct Note: Enter at runtime.
	Instance Password	DomainUserPswd Note: Enter at runtime.

Be sure that the default values for all remaining parameters are appropriate for your environment (see ["Parameters for Restore MS SQL Database" on the next page](#)).

Parameters for Restore MS SQL Database

The following tables describe the required and optional input parameters for this workflow. Most of these parameters are not initially visible in a deployment. For most parameters, if you do not specify a value for a parameter, a default value is assigned

Parameters Defined in this Step: Gather Parameters for MS SQL Database Restore

Parameter Name	Default Value	Required	Description
Database Backup File	no default	required	<p>Path where the database backup file is (or will be) stored, either locally or on a network share.</p> <p>If the file already exists locally or on a network share, specify the file name in this parameter and the path in the Download Target Destination parameter.</p> <p>If the file does not yet exist locally or on a network share, it will be downloaded into this location from the software repository.</p> <p>If the file is (or will be) stored on a network share, the Windows Share User must have read and write access to that share.</p>
Download Target Destination	no default	required	<p>The directory where the database backup file will be stored.</p> <p>If the database backup file does not yet exist in this directory, it will be downloaded from the software repository and stored in this directory.</p>

Additional Parameters Defined in this Step: Gather Advanced Parameters for MS SQL Database Restore

Parameter Name	Default Value	Required	Description
Backup Encryption Password	no default	optional	To decrypt a backup file that was encrypted with a password, specify the password in this parameter.
Data File Locations	no default	optional	<p>Comma-delimited list of directories or full file paths for each data file in the backup file.</p> <p>Use Run Simulation Only mode to discover the number of data files in the backup file. If this parameter is not specified, the original data file names and paths will be used.</p>
Database Name	no default	optional	To restore the database from the backup file using a different database name, specify that name here. If this parameter is not specified, the original database name will be used.
Instance Account	no default	optional	The Windows account that will perform the restore operation.
Instance Password	no default	optional	The password for the Windows account that will perform the restore operation.
Log File Locations	no default	optional	Comma-delimited list of directories or full file paths for each log file in the backup file. Use Run Simulation Only mode to discover the number of log files in backup file. If this parameter is not specified, the original log file names and paths will be used.

Additional Parameters Defined in this Step: Gather Advanced Parameters for MS SQL Database Restore , continued

Parameter Name	Default Value	Required	Description
Overwrite Existing Database	NO	optional	If set to YES, and the database already exists, the workflow will overwrite the database. Valid values: YES or NO. If set to NO, and the database already exists, the workflow will fail.
Preserve Users and Roles	NO	optional	If set to YES, and the database already exists, the workflow will try to preserve the database users and role. Valid values: YES or NO.
Reindex Restored Database	NO	optional	If set to YES, the workflow will re-index the database after the restore operation is successfully completed. Valid values: YES or NO. Re-indexing improves database performance. More specifically , it recreates all the table look-ups and performance tunes them according to the new environment. This is important when you are restoring a database in a new environment that it has never seen before.
Run Simulation Only	NO	optional	If set to YES, the workflow will only run the Pre-Restore Validation step. It will not attempt to restore the database. Use this mode to discover the original data and log files used for the database backup. Valid values: YES or NO.

MS SQL - Backup and Restore Database

This workflow enables you to backup the contents of a SQL Server database (the **source database**) into a file and restore a database in another instance (the **target instance**) using the contents of that backup file. The source database and target instance are specified at run time.

This is a **bridged execution** workflow. The first group of steps performs the backup on the specified source database. The second group of steps performs the restore on the specified database in the specified target instance.

You can specify various options, including whether the backup file is compressed or encrypted with a password.

Note: Bridged execution workflows work on one target level (server, instance, or database). This workflow runs on the database level at all times. When choosing a target instance at run time, you will actually see a list of databases that reside on each instance. You can select any database in the target instance where you want to perform the restore.

If you specify the RESTORE - Database Name parameter, the workflow will use that database. If you do not specify the RESTORE - Database Name parameter, the workflow will use the original database name from the backup.

If the database specified in the Database Name parameter does not exist in the target instance, the workflow will create it. If the database already exists, you can specify whether you want the workflow to overwrite its contents. You can also specify whether existing database users should be re-created after the restore operation—in which case, any users included in the backup file are ignored .

This workflow also provides a "simulation mode" where the Run MS SQL Pre-Restore Validation step is executed, but the restore is not performed. This is useful for testing or troubleshooting your parameter values.

The workflow performs extensive validation checks prior to and immediately after both the backup and restore operations to ensure that both the backup file and the restored database are valid.

See ["Parameters for Backup and Restore MS SQL Database" on page 627](#) for a list of backup and restore options that you can specify. Many of these parameters are hidden by default

The process of deploying and running this workflow is the same for all scenarios, but the parameters required will differ depending on the specific scenario that you are implementing.

The workflow provides default values for most parameters. These default values are usually sufficient for a "typical" database refresh. You can override the defaults by specifying parameter values in the deployment. You can also expose additional parameters in the workflow, if necessary, to accomplish more advanced scenarios.

Topic	Information Included
"Prerequisites for this Workflow"	List of prerequisites that must be satisfied before you can run this workflow
"How this Workflow Works"	Information about what the workflow does, including validation checks performed, steps executed, and a high-level process flow
"How to Run this Workflow"	Instructions for running this workflow in your environment
"Sample Scenarios"	Examples of typical parameter values for this workflow
"Parameters for Backup and Restore MS SQL Database"	List of input parameters for this workflow

The process of deploying and running this workflow is the same for all scenarios, but the parameters required will differ depending on the specific scenario that you are implementing.

The workflow provides default values for most parameters. These default values are usually sufficient for a "typical" database backup and restore. You can override the defaults by specifying parameter values in the deployment. You can also expose additional parameters in the workflow, if necessary, to accomplish more advanced scenarios.

Any parameters not explicitly specified in the deployment will have the default values listed in ["Parameters for Backup and Restore MS SQL Database" on page 627](#) .

Prerequisites for this Workflow

The following prerequisites must be satisfied before you can run the ["MS SQL - Restore Database"](#) workflow:

1. The service login for the SQL Server service must have read and write permissions on the location where the backup file will be stored.
2. The server management agent must have login access to the target SQL Server instance. It must also have permission to create a new database and perform database consistency check (DBCC) commands on the restored database.
3. There must be sufficient space available to create the backup file and restore the database (including both data and logs). The workflow checks for this, and will fail if sufficient space is not available.

Additional Considerations

For information about prerequisites for SQL Server, refer to the [SQL Server Product Documentation](#).

How this Workflow Works

This topic contains information about the "[MS SQL - Backup and Restore Database](#)" workflow:

Validation Checks Performed

The workflow checks the following things prior to dumping the database. If any of these checks fails, the workflow fails.

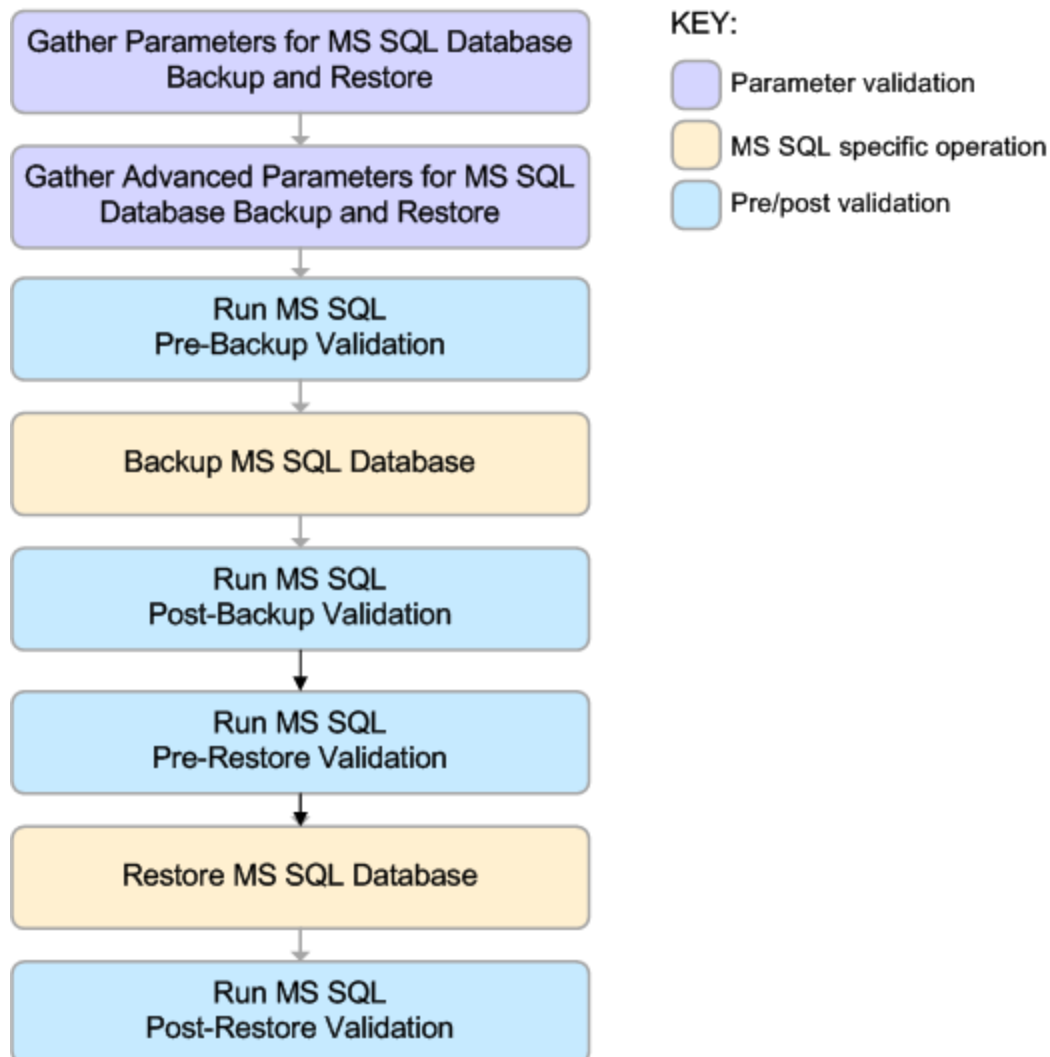
1. All required parameters have values. If any required parameter does not have a value—either a value that you specify or a default value—the workflow fails in either the Run MS SQL Pre-Backup Validation step or the Run MS SQL Pre-Restore Validation step.
2. The Working Path is accessible, either locally or on a network share.

If the Working Path is on a network share, the BACKUP - Windows Share User has read and write access the share.
3. The source database is compatible with the target instance.
4. If the RESTORE - Database Name parameter is specified, this database name complies with SQL Server database naming conventions.
5. The target instance exists, and the workflow can connect to it.
6. Adequate disk space is available to backup and restore the data and log files.

Steps Executed

The "MS SQL - Backup and Restore Database" workflow includes the following steps. Each step must complete successfully before the next step can start. If a step fails, the workflow reports a failure, and all subsequent steps are skipped.

Click each box in the diagram to view additional information about that step in a new window.



Process Flow

This workflow performs the following tasks:

1. Performs the preliminary [validation checks](#) described above.
2. If RESTORE - Preserve Users and Roles was set to YES, creates the Roles Creation and Users Creation scripts.
3. Performs the database backup operation to create the backup file.
4. Performs post-backup validation checks to ensure that all required parameters had valid values.
5. If BACKUP - Perform Integrity Check was set to YES, performs an integrity check on the backup file.
6. If not in simulation mode, performs the database restore operation to load the contents of the backup file.
7. Performs post-restore validation checks to ensure that the restored database is sound.
8. If RESTORE - Preserve Users and Roles was set to YES, re-creates any existing database users and roles.
9. If RESTORE - Reindex Restored Database was set to YES, re-indexes the database.

Tips and Best Practices

It is good practice to run basic database consistency checks (DBCCs) on the source database before you create the database backup to ensure that there are no internal errors in the database.

If you find errors in the source database, be sure to fix them before you run this workflow. This workflow does not have the ability to diagnose or remediate problems in the database prior to performing the database backup.

How to Run this Workflow

This topic explains how to customize and run the "MS SQL - Backup and Restore Database" workflow in your environment.

Note: Prior to running this workflow, review the "Prerequisites for this Workflow", and ensure that all requirements are satisfied.

To customize and run the Backup and Restore MS SQL Database workflow:

11. Create a deployable copy of the workflow.
2. Determine the values that you will specify for the following parameter. This is the minimum set of parameters required to run this workflow.

Parameter Name	Default Value	Description
Working Path	no default	<p>The directory where the database backup file will be stored. This can be a directory or a full file path. This path must be accessible to both the source and target servers.</p> <p>Be sure to specify this parameter in network share notation (for example: \\<network share>\). A network path can be located on a target server, but it should always be referenced using network share notation instead of local folder notation (for example: C:\<folder>).</p> <p>You specify this parameter in the deployment.</p>

See "Parameters for Backup and Restore MS SQL Database" on page 627 for detailed descriptions of all input parameters for this workflow, including default values.

3. In the workflow editor, expose any additional parameters that you need. You will specify values for these parameters when you create the deployment or at runtime.
4. Save the changes to the workflow (click **Save** in the lower right corner).
5. Create a new deployment.
 - a. On the Targets tab, select all the target servers—both source and destination—that will participate in this database refresh. The targets that you select here will be available in the Target Parameters drop-down menus on the Run page (see [step 7](#)).
 - b. On the Parameters tab, specify values (or set the type to Runtime Value) for the required parameters listed in [step 2](#) and any additional parameters that you exposed in [step 3](#). You do

not need to specify values for those parameters whose default values are appropriate for your environment.

6. Save the deployment (click **Save** in the lower right corner).
7. Run the workflow using this deployment, specifying any runtime parameters .

On the Run page, select the following targets from the respective drop-down menus:

Parameter Name	Default	Description
Source Database	no default	The database from which the backup file will be created. You specify this parameter at run time.
Target Instance	no default	<p>The instance where the database will be restored from the backup file. You specify this parameter at run time.</p> <p>Note: Bridged execution workflows work on one target level (server, instance, or database). This workflow runs on the database level at all times. When choosing a target instance at run time, you will actually see a list of databases that reside on each instance. You can select any database in the target instance where you want to perform the restore.</p> <p>If you specify the RESTORE - Database Name parameter, the workflow will use that database. If you do not specify the RESTORE - Database Name parameter, the workflow will use the original database name from the backup.</p>

The workflow will complete and report “Success” on the Console if it has run successfully. If an invalid parameter value is specified, an error is logged, and the workflow terminates in the “Failure” state.

Sample Scenarios

This topic shows you how to use various parameters to achieve the following database backup scenarios in your environment using the ["MS SQL - Backup and Restore Database"](#) workflow:

Scenario 1: Backup and Restore Using a Backup File that is Not Encrypted or Compressed

This is the simplest SQL Server database backup and restore scenario. In this example, the backup file is stored on a network share.

Step Name	Parameter Name	Example Value
Gather Parameters for MS SQL Database Backup and Restore	Source Database	Specified at run time.
	Target Instance	Specified at run time.
	Working Path	\\WIN-DOMAIN-CTRL\Backups

Scenario 2: Backup and Restore—Overwrite Existing Database and Preserve Existing Users

This scenario requires you to specify the two restore parameters that instruct the workflow to overwrite the existing database and then re-create existing users and roles. In this example, the backup file is stored on a network share.

Note that the BACKUP - Windows Share User and BACKUP - Windows Share Password are specified. This is not required, but it facilitates the disk space check on the network path. If you do not specify this parameter, this check is skipped.

Step Name	Parameter Name	Example Value
Gather Parameters for MS SQL Database Backup and Restore	Source Database	Selected at run time.
	Target Instance	Selected at run time.
	Working Path	\\WIN-DOMAIN-CTRL\Backups
Gather Advanced Parameters for MS SQL Database Backup and Restore	BACKUP - Windows Share User	WIN\Administrator
	BACKUP - Windows Share Password	WinSharePwd
	RESTORE - Overwrite Existing Database	YES
	RESTORE - Preserve Users and Roles	YES

Scenario 3: Perform a Backup, Simulate a Restore, and Configure Windows Domain User Using Runtime Parameters

This scenario overwrites an existing database and restores any existing users after the restore is performed. In this example, the backup file is stored on a network share.

Note: You may want to run this workflow against a MS SQL instance that can only be accessed by a Windows user with a temporary password. By using a runtime parameter for the password, you can ensure that the password used is always the latest.

To specify the Windows domain user at the time you execute a deployment with runtime parameters, perform the following additional steps:

1. When you make a copy of the workflow, expand the appropriate step, and then set the following Windows domain user parameters to - **User selected** -:

 BACKUP - Instance Account
 BACKUP - Instance Password
 RESTORE - Instance Account
 RESTORE - Instance password
2. When you create a deployment from the copy of the workflow, set the parameter types to **Runtime Value**.
3. When you execute the deployment, specify the Windows domain user account and password.

Step Name	Parameter Name	Example Value
Gather Parameters for MS SQL Database Backup and Restore	Source Database	Selected at run time.
	Target Instance	Selected at run time.
	Working Path	\\WIN-DOMAIN-CTRL\Backups
Gather Advanced Parameters for MS SQL Database Backup and Restore	BACKUP - Windows Share User	WIN\Administrator
	BACKUP - Windows Share Password	WinSharePwd Tip: To avoid having to re-enter passwords whenever they change, you can create a policy to provide them to the workflow.
	ALL - Run Simulation	YES

Step Name	Parameter Name	Example Value
	Only	
	BACKUP - Instance Account	Domain\DomainUserAcct Note: Enter at runtime.
	BACKUP - Instance Password	DomainUserPswd Note: Enter at runtime.
	RESTORE - Instance Account	Domain\DomainUserAcct Note: Enter at runtime.
	RESTORE - Instance Password	DomainUserPswd Note: Enter at runtime.

Be sure that the default values for all remaining parameters are appropriate for your environment (see Parameters for Backup and Restore MS SQL Database).

Parameters for Backup and Restore MS SQL Database

The following tables describe the required and optional input parameters for this workflow. Most of these parameters are not initially visible in a deployment. For most parameters, if you do not specify a value for a parameter, a default value is assigned

Parameters Defined in this Step: Gather Parameters for Backup and Restore MS SQL Database

Parameter Name	Default Value	Required	Description
Source Database	no default	required	The database from which the backup file will be created. You specify this parameter at run time.
Target Instance	no default	required	The instance where the database will be restored from the backup file. You specify this parameter at run time. Note: Bridged execution workflows work on one target level (server, instance, or database). This workflow runs on the database level at all times. When choosing a target instance at run time, you will actually see a list of databases that reside on each instance. You can select any database in the target instance where you want to perform the restore. If you specify the RESTORE - Database Name parameter, the workflow will use that database. If you do not specify the RESTORE - Database Name parameter, the workflow will use the original database name from the backup.
Working Path	no default	required	The directory where the database backup file will be stored. This can be a directory or a full file path. This path must be accessible to both the source and target servers. Be sure to specify this parameter in network share notation (for example: \\<network share>\). A network path can be located on a target server, but it should always be referenced using network share notation instead of local folder notation (for example: C:\<folder>). You specify this parameter in the deployment.

Additional Parameters Defined in this Step: Gather Advanced Parameters for Backup and Restore MS SQL Database

Parameter Name	Default Value	Required	Description
ALL - Encryption Password	no default	optional	Password used to encrypt and decrypt the backup file. To decrypt a backup file that was encrypted with a password, specify the password in this parameter.

Additional Parameters Defined in this Step: Gather Advanced Parameters for Backup and Restore MS SQL Database, continued

Parameter Name	Default Value	Required	Description
ALL - Run Simulation Only	No	optional	If set to YES, the workflow will only run the Pre-Restore Validation step. It will not attempt to restore the database. Use this mode to discover the original data and log files used for the database backup. Valid values: YES or NO.
BACKUP - Backup Description	no default	optional	Text that describes this backup (up to 255 characters).
BACKUP - Backup Name	no default	optional	The name of this backup (up to 128 characters).
BACKUP - Compress Backup File	NO	optional	<p>If you specify YES, the backup file will be compressed. Valid values: YES or NO.</p> <p>Compression is supported on SQL Server 2008 Enterprise and later.</p>
BACKUP - Expiration Date	no default	optional	<p>Date and time when the backup file expires and the backup data is no longer considered relevant. After this date and time, SQL Server is not prevented from overwriting this backup file.</p> <p>The Expiration Date must be specified in a format compatible with the configured system datetime format.</p> <p>If both the Retention Days and the Expiration Date parameters are specified, the Retention Days parameter takes precedence.</p>
BACKUP - Instance Account	no default	optional	The Windows account that will perform the backup operation.
BACKUP - Instance Password	no default	optional	The password for the Windows account that will perform the backup

Additional Parameters Defined in this Step: Gather Advanced Parameters for Backup and Restore MS SQL Database, continued

Parameter Name	Default Value	Required	Description
			operation.
BACKUP - Perform Integrity Check	NO	optional	If you specify YES, the workflow will perform an integrity check on the database backup file. Valid values: YES or NO.
BACKUP - Retention Days	no default	optional	<p>Number of days that must elapse before this backup file can be overwritten by SQL Server.</p> <p>If both the Retention Days and the Expiration Date parameters are specified, the Retention Days parameter takes precedence.</p>
BACKUP - Windows Share Password	no default	optional	Password for the user specified in Windows Share User.
BACKUP - Windows Share User	no default	optional	Windows user who can access the specified Windows network share and who will own (and write) the backup file.
RESTORE - Data File Locations	no default	optional	<p>Comma-delimited list of directories or full file paths for each data file in the backup file.</p> <p>Use Run Simulation Only to discover the number of data files in backup file. If this parameter is not specified, the original data file name will be used.</p>
RESTORE - Database Name	no default	optional	To restore the database from the backup file using a different database name, specify that name here. If this parameter is not specified, the original database name will be used.
RESTORE - Download Target Destination	no default	optional	The directory where the database backup file will be stored.
RESTORE - Instance Account	no	optional	The Windows account that

Additional Parameters Defined in this Step: Gather Advanced Parameters for Backup and Restore MS SQL Database, continued

Parameter Name	Default Value	Required	Description
	default		will perform the restore operation.
RESTORE - Instance Password	no default	optional	The password for the Windows account that will perform the restore operation.
RESTORE - Log File Locations	no default	optional	Comma-delimited list of directories or full file paths for each log file in the backup file. Use Run Simulation Only mode to discover the number of log files in backup file. If this parameter is not specified, the original log file name will be used.
RESTORE - Overwrite Existing Database	NO	optional	If set to YES, and the database already exists, the workflow will overwrite the database. Valid values: YES or NO.
RESTORE - Preserve Users and Roles	NO	optional	If set to YES, and the database already exists, the workflow will overwrite the database. Valid values: YES or NO.
RESTORE - Reindex Restored Database	NO	optional	<p>If set to YES, the workflow will re-index the database after the restore operation is successfully completed. Valid values: YES or NO.</p> <p>Re-indexing improves database performance. More specifically, it recreates all the table look-ups and performance tunes them according to the new environment. This is important when you are restoring a database in a new environment that it has never seen before.</p>

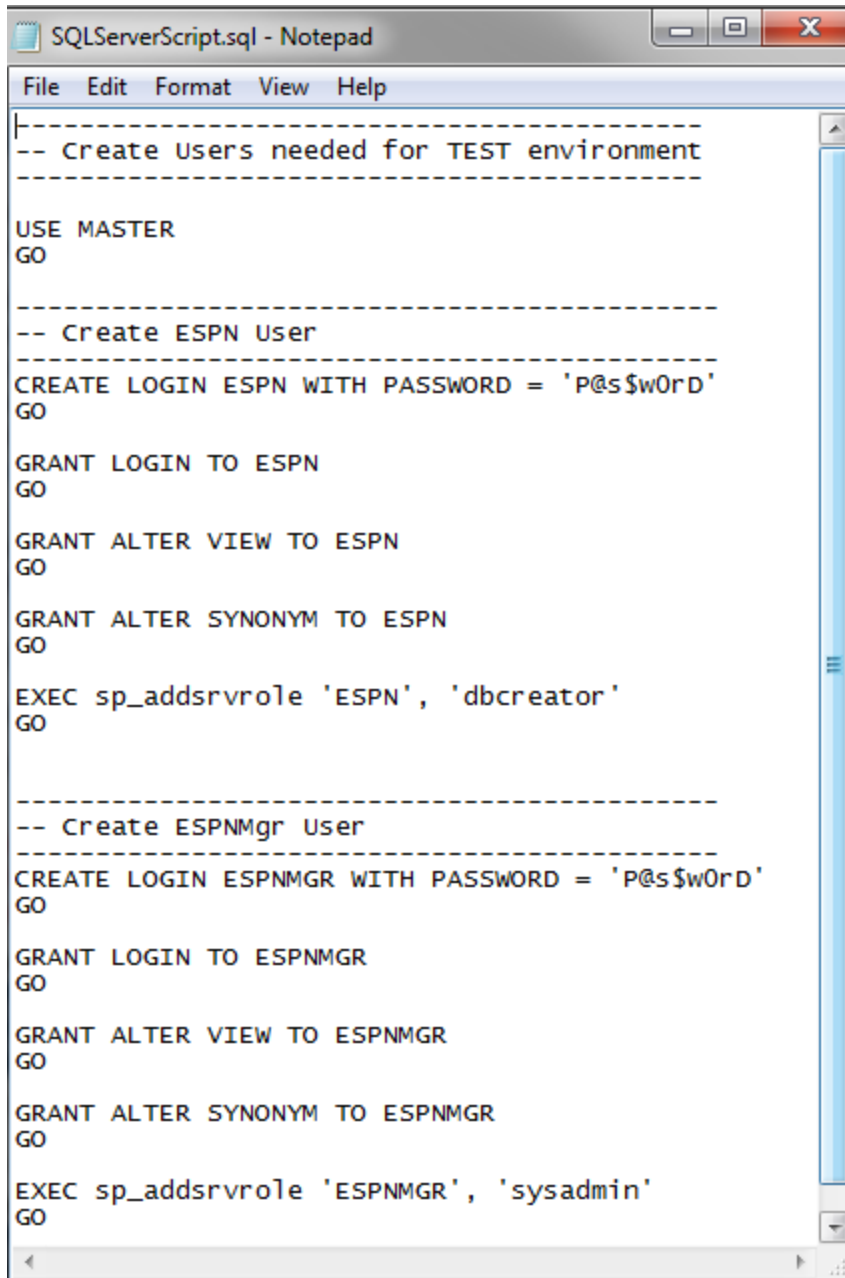
DB Release for SQL Server v2

This workflow will check a list of T-SQL script and embedded SQL files for disallowed commands, check the syntax, then execute the files on the targetMicrosoft SQL Server Microsoft SQL Server databases if they pass all required tests.

This workflow is designed for SQL script transactions to be deployed and executed against target SQL Server databases. SQL scripts are stored and downloaded from the DMA software repository.

If the SQL scripts are embedded within a SQL script, this workflow has the ability to download the embedded scripts from SA core, provided the location of the sub-script is same as the staging directory. This workflow can download only one level of embedded SQL scripts.

Before running the DB Release for SQL Server workflow you need to create the SQL script file (or files). For example:



```
SQLServerScript.sql - Notepad
File Edit Format View Help
-----
-- Create Users needed for TEST environment
-----

USE MASTER
GO

-----
-- Create ESPN User
-----

CREATE LOGIN ESPN WITH PASSWORD = 'P@s$w0rD'
GO

GRANT LOGIN TO ESPN
GO

GRANT ALTER VIEW TO ESPN
GO

GRANT ALTER SYNONYM TO ESPN
GO

EXEC sp_addsrvrole 'ESPN', 'dbcreator'
GO

-----
-- Create ESPNMGR User
-----

CREATE LOGIN ESPNMGR WITH PASSWORD = 'P@s$w0rD'
GO

GRANT LOGIN TO ESPNMGR
GO

GRANT ALTER VIEW TO ESPNMGR
GO

GRANT ALTER SYNONYM TO ESPNMGR
GO

EXEC sp_addsrvrole 'ESPNMGR', 'sysadmin'
GO
```

You can customize what the workflow checks in the SQL scripts:

- SQL advanced features
- SQL database commands
- SQL database links
- SQL syntax
- SQL system grants
- A regular expression

If all the tests pass, the SQL scripts may be deployed and executed against the target SQL Server databases.

Note: This workflow does not provide any rollback capability.

To use this workflow in your environment, see the following information:

Topic	Information Included
"Prerequisites for this Workflow" on the next page	List of prerequisites that must be satisfied before you can run this workflow
"How this Workflow Works" on page 635	Information about what the workflow does, including validation checks performed, and steps executed
"How to Run this Workflow" on page 638	Instructions for running this workflow in your environment
"Sample Scenarios" on page 642	Examples of typical parameter values for this workflow
"Parameters for DB Release for SQL Server v2" on page 645	List of input parameters for this workflow

Prerequisites for this Workflow

Be sure that the following prerequisites are satisfied before you run the ["DB Release for SQL Server v2"](#) workflow.

Dependencies

- This solution requires DMA version 10.50 (or later).

The latest DMA solution packs require the latest DMA platform. To use the latest solution packs, update the DMA platform. DMA10.50.001.000 solution packs are supported on DMA10.50.001.000 (and later).
- You have installed the Database Compliance solution pack.
- An SQL Server instance and its databases should already be provisioned and added to the Environment section—this can be accomplished by using Discovery.
- The SQL scripts must be available in the DMA software repository.
- You have installed the `osql` or `SQLCMD` utility and made it accessible via the user/password settings stored in the metadata. Check the Environment page for those settings. If there is no metadata, the connection will use Windows authentication.
- You need an SA (System Administrator) role to perform any server level or database level updates.

Supported Versions of SQL Server

2008, 2008 R2, 2012, 2014

SQL Scripts

You need to create the SQL scripts that manage the release. The files may contain the normal SQL Server DML and DDL commands.

Tip: List the SQL scripts in the SQL scripts parameter in the order in which they need to be executed.

SQL Server Documentation

For more information about prerequisites for SQL Server, refer to the [Microsoft SQL Server Documentation](#).

How this Workflow Works

The following information describes how the "DB Release for SQL Server v2" workflow works.

Overview

The workflow starts by gathering input parameters.

If the SQL scripts do not exist on the specified target location, they are downloaded from the software repository.

Based on the parameters you set when you create your deployment, the workflow will do the following:

- Check the SQL code for SQL advanced features—unless specified in the exception list. If any are found, the workflow will exit with a failure code.
- Check the SQL code for SQL database commands—unless specified in SQL commands to be excluded from the check. If any are found, the workflow will exit with a failure code.
- Check the SQL code for any SQL database links—if any are found, the workflow will exit with a failure code.
- Check the SQL code for syntax errors—if any are found, the workflow will exit with a failure code.
- Check the SQL code for any SQL system grants—unless specified in the exception list. If any are found, the workflow will exit with a failure code.
- Check the SQL code for a regular expression that you specify—if any matches are found, the workflow will exit with a failure code.

If there were no errors in the checks and the Run Flag is set, the workflow uses the `osql` or `SQLCMD` utility to execute the SQL script files.

Validation Checks Performed

This workflow validates the SQL scripts in the following ways:

1. If you set the Run Flag to Check SQL Advanced Features, the workflow searches for any instance configuration options—unless included in your exclusion list. These are instance level settings that most users shouldn't be changing, for example, startup procs and xp_cmdshell.
2. If you set the Run Flag to Check SQL Database Commands, the workflow searches the SQL statements for the commands that you specify in SQL Commands.
3. If you set the Run Flag to Check SQL Database Links, the workflow searches the SQL statements for OPENQUERY, OPENROWSET, and OPENDATASOURCE statements. It also checks for this pattern: [server].[instance].[owner].[database]
4. If you set the Run Flag to Check SQL Syntax, the workflow verifies that all the SQL statements have valid syntax.
5. If you set the Run Flag to Check SQL System Grants, the workflow searches the SQL statements for any system level (server role) grants—unless included in your exclusion list. For example:
GRANT CONTROL SERVER TO SOMEUSER
6. If you set the Run Flag to Match Regular Expression to SQL Server Scripts and you specify a regular expression, the workflow searches the SQL statements for any regex matches.

If any of the validations fail, the workflow will output the offending SQL line to stdout, return an error status, and the SQL scripts will not be executed.

Steps Executed

The "DB Release for SQL Server v2" workflow includes the following steps. Each step must complete successfully before the next step can start. If a step fails, the workflow reports a failure and all subsequent steps are skipped.

Steps Used in DB Release for SQL Server

Workflow Step	Description
MS SQL - Parameters - DB Release for SQL Server	This step accepts the basic input parameters for the workflow. The parameters will be used in subsequent steps.
Check if Download File Exists	This step determines whether one or more specified files already exist on the target server.
Check For Nested SQL files in MSSQL SQL file	This step checks for embedded SQL scripts.
Download Software	This step downloads a list of files to a specified location on the target server.
Check SQL Advanced	This step checks the SQL scripts for any advanced feature non-default

Steps Used in DB Release for SQL Server, continued

Workflow Step	Description
Features	setting. An exception list can be specified to exclude specific advanced features from the check.
Check SQL Database Commands	This step checks the SQL scripts to ensure that specific types of SQL database commands—as specified in the SQL Commands parameter—are not included.
Check SQL Database Links	This step checks an SQL Script for any database link usage.
Check SQL System Grants	This step checks an SQL Script for any system level (server role) grants. An exception list can be specified to exclude specific privileges from the check.
Match Regular Expression to SQL Server Scripts	This step applies a regular expression to each SQL statement in an SQL Script file. If any <code>regex</code> matches are found, they are output to <code>stdout</code> and an error is returned.
Check SQL Syntax	This step verifies the syntax of an SQL Server Script. The step assumes that a <code>go</code> statement on its own line signifies the end of a code block.
Run SQL Server Script v2	This step executes SQL Scripts using <code>osql.exe</code> . This step is only executed if all the previous checks passed.

Note: For input parameter descriptions and defaults, see ["Parameters for DB Release for SQL Server v2" on page 645](#).

How to Run this Workflow

The following instructions show you how to customize and run the ["DB Release for SQL Server v2"](#) workflow in your environment.

The workflow provides default values for some parameters. These default values are usually sufficient for a "typical" installation. You can override the defaults by specifying parameter values in the deployment. You can also expose additional parameters in the workflow, if necessary, to accomplish more advanced scenarios. Any parameters not explicitly specified in the deployment will have the default values listed in ["Parameters for DB Release for SQL Server v2" on page 645](#).

Note: Before following this procedure, review the ["Prerequisites for this Workflow" on page 634](#), and ensure that all requirements are satisfied.

To use the DB Release for SQL Server workflow:

1. Create a deployable copy of the workflow.
2. Determine the values that you will specify for the following parameters:

Input Parameters for MS SQL - Parameters - DB Release for SQL Server

Parameter Name	Default Value	Required	Description
Display SQL Length	2000	optional	The number of characters of a SQL batch that is displayed when an error occurs. Enter "0" to display the entire code. Note: Displaying the entire code may cause performance issues for your browser.
File List	no default	required	Comma-separated list of the files that contain the SQL scripts that will be checked. Note: List the SQL script files in the order in which they need to be executed.
Staging Directory	C:\Temp\	optional	The directory that contains the SQL scripts that will be checked.

Input Parameters for Check SQL Advanced Features

Parameter Name	Default Value	Required	Description
Exception List	see description	optional	Comma-separated list of advanced features that will be allowed. For example, if you specify CURSOR THRESHOLD, QUERY WAIT, those advanced features will be allowed—any other

Input Parameters for Check SQL Advanced Features, continued

Parameter Name	Default Value	Required	Description
			advanced features that occur in the code will cause the workflow to fail. The default is to check all of the normal advanced features.
Run Flag	Y	optional	Flag to indicate whether the workflow should run this check. Valid values are Y (run the check) or N (do not run the check).

Input Parameters for Check SQL Database Commands

Parameter Name	Default Value	Required	Description
Run Flag	Y	optional	Flag to indicate whether the workflow should run this check. Valid values are Y (run the check) or N (do not run the check).
SQL Commands	shutdown, sp_configure, create database, drop database, create login, create user, drop login, drop user, sp_grantdbaccess, sp_addlogin, sp_droplogin	optional	Comma-separated list of SQL commands that are not allowed. The default shows an example of how to fill out the list. You may want to customize this list for your configuration.

Input Parameters for Check SQL Database Links

Parameter Name	Default Value	Required	Description
Run Flag	Y	optional	Flag to indicate whether the workflow should run this check. Valid values are Y (run the check) or N (do not run the check).

Input Parameters for Check SQL Syntax

Parameter Name	Default Value	Required	Description
Run Flag	Y	optional	Flag to indicate whether the workflow should run this check. Valid values are Y (run the

Input Parameters for Check SQL Syntax, continued

Parameter Name	Default Value	Required	Description
			check) or N (do not run the check).

Input Parameters for Check SQL System Grants

Parameter Name	Default Value	Required	Description
Exception List	grant db_owner, grant ddladmin, grant sysadmin, grant securityadmin, grant serveradmin, grant processadmin, grant diskadmin, grant dbcreator	optional	Comma-separated list of SQL system privileges that will be allowed. For example, if you specify , those system privileges will be allowed—any other system privileges that occur in the code will cause the workflow to fail. The default shows an example of how to fill out the list. You may want to customize this list for your configuration.
Run Flag	Y	optional	Flag to indicate whether the workflow should run this check. Valid values are Y (run the check) or N (do not run the check).

Input Parameters for Match Regular Expression to SQL Server Scripts

Parameter Name	Default Value	Required	Description
Regular Expression		optional	The regular expression to be searched for in all of the SQL scripts to be deployed. If the specified regular expression is found, the workflow exits with a failure. For example: drop\s+table will match all statements that drop a table.
Run Flag	Y	optional	Flag to indicate whether the workflow should run this check. Valid values are Y (run the check) or N (do not run the check).

Input Parameters for Run SQL Server Script

Parameter Name	Default Value	Required	Description
Database Name	master	optional	The name of the database to which the specified SQL scripts will be applied.
Run Flag	Y	optional	Flag to indicate whether the workflow should run the SQL Server script. Valid values are Y (run the check) or N (do not run the check).

Note: See ["Parameters for DB Release for SQL Server v2" on page 645](#) for detailed descriptions of all input parameters for this workflow, including default values.

3. In the workflow editor, expose any additional parameters that you need. You will specify values for those parameters when you create the deployment or at runtime.
4. Save the changes to the workflow (click **Save** in the lower right corner).
5. Create a new deployment.
6. On the Parameters tab, specify values (or set the type to Runtime Value) for the required parameters listed in step 2 and any additional parameters that you have exposed. You do not need to specify values for those parameters whose default values are appropriate for your environment.
7. On the Targets tab, specify one or more targets for this deployment.
8. Save the deployment (click **Save** in the lower right corner).
9. Run the workflow using this deployment, specifying any runtime parameters.

To verify the results:

The workflow will complete and report SUCCESS on the Console if it has run successfully. If an error occurs during workflow execution, the error is logged, and the workflow terminates in the FAILURE state.

Optional: If you want to further verify the results:

Log in to your database to make sure that whatever you created or modified was actually done.

To view the output:

The workflow writes the execution output for SQL script execution in the DMA Steplog.

Sample Scenarios

This topic shows you typical parameter values for different use cases for the ["DB Release for SQL Server v2"](#) workflow.

Scenario 1: Check the SQL script files for disallowed commands, check the syntax, then deploy and execute the scripts

You only need to specify the File List and the Staging Directory since this scenario takes advantage of many parameter defaults. The workflow will check the SQL script files for:

- All of the normal advanced features
- All of the SQL database commands that are in the default SQL Commands parameter
- SQL database links
- SQL syntax
- All the SQL system grants—except those in the default Exception List parameter
- No regular expression—since none is specified by default

As long as no error is discovered in the checks, the SQL scripts will be deployed and executed on the target SQL Server databases.

Determine the values that you will specify for the following parameters:

Input Parameters for MS SQL - Parameters - DB Release for SQL Server

Parameter Name	Example Value	Description
File List	sqlserverscript.sql	Comma-separated list of the files that contain the SQL scripts that will be checked. Note: List the SQL script files in the order in which they need to be executed.
Staging Directory	C:\Temp\	The directory that contains the SQL scripts that will be checked.

Be sure that the default values for all remaining input parameters are appropriate for your environment (see ["Parameters for DB Release for SQL Server v2" on page 645](#)).

Scenario 2: Check the SQL script files for disallowed commands, check the syntax, configure Windows domain user using runtime parameters, but do not deploy and execute the scripts

This scenario takes advantage of many parameter defaults and also demonstrates some optional parameters. The workflow will check the SQL script files for:

- All of the SQL database commands that are in the default SQL Commands parameter
- SQL database links
- SQL syntax
- All the SQL system grants—except those in the default Exception List parameter
- The regular expression drop\s+table
- A database to which the SQL scripts will be applied

Note: You may want to run this workflow against a MS SQL instance that can only be accessed by a Windows user with a temporary password. By using a runtime parameter for the password, you can ensure that the password used is always the latest.

To specify the Windows domain user at the time you execute a deployment with runtime parameters, perform the following additional steps:

1. When you make a copy of the workflow, expand the appropriate step, and then set the Windows domain user parameters—Instance Account and Instance Password—to **- User selected -**.
2. When you create a deployment from the copy of the workflow, set the parameter types to **Runtime Value**.
3. When you execute the deployment, specify the Windows domain user account and password.

This workflow run will only report the results of the checks. The SQL scripts will NOT be deployed and executed on the target SQL Server databases.

Determine the values that you will specify for the following parameters:

Input Parameters for MS SQL - Parameters - DB Release for SQL Server

Parameter Name	Example Value	Description
File List	sqlserverscript.sql	Comma-separated list of the files that contain the SQL scripts that will be checked. Note: List the SQL script files in the order in which they need to be executed.

Input Parameters for MS SQL - Parameters - DB Release for SQL Server, continued

Parameter Name	Example Value	Description
Instance Account	Domain\DomainUserAcct Note: Enter at runtime.	The Windows account that will perform the release management.
Instance Password	DomainUserPswd Note: Enter at runtime.	The password for the Windows account that will perform the release management.
Staging Directory	C:\Temp\	The directory that contains the SQL scripts that will be checked.

Input Parameters for Match Regular Expression to SQL Server Scripts

Parameter Name	Example Value	Description
Regular Expression	drop\s+table	The regular expression to be searched for in all of the SQL scripts to be deployed. If the specified regular expression is found, the workflow exits with a failure. For example: drop\s+table will match all statements that drop a table.
Run Flag	Y	Flag to indicate whether the workflow should run this check. Valid values are Y (run the check) or N (do not run the check).

Input Parameters for Run SQL Server Script

Parameter Name	Example Value	Description
Database Name	mydb	The name of the database to which the specified SQL scripts will be applied.
Run Flag	N	Flag to indicate whether the workflow should run the SQL Server script. Valid values are Y (run the check) or N (do not run the check).

Note: Some of these parameters are not exposed by default in the deployment.

Be sure that the default values for all remaining input parameters are appropriate for your environment (see ["Parameters for DB Release for SQL Server v2" on the next page](#)).

Parameters for DB Release for SQL Server v2

The following tables describe the required and optional input parameters for this workflow. Some of these parameters may not be initially visible in a deployment. For some parameters, if you do not specify a value for a parameter, a default value is assigned.

Note: Only those parameters that are configurable in a standard deployment are listed here. Input parameters that must be mapped to output parameters of previous steps are not listed.

Input Parameters Defined in this Step: MS SQL - Parameters - DB Release for SQL Server

Parameter Name	Default Value	Required	Description
Display SQL Length	2000	optional	The number of characters of a SQL batch that is displayed when an error occurs. Enter "0" to display the entire code. Note: Displaying the entire code may cause performance issues for your browser.
File List	no default	required	Comma-separated list of the files that contain the SQL scripts that will be checked. Note: List the SQL script files in the order in which they need to be executed.
Instance Account	no default	optional	The Windows account that will perform the release management.
Instance Password	no default	optional	The password for the Windows account that will perform the release management.
Staging Directory	C:\Temp\	optional	The directory that contains the SQL scripts that will be checked.

Additional Input Parameters Defined in this Step: Check SQL Advanced Features

Parameter Name	Default Value	Required	Description
Exception List	see description	optional	Comma-separated list of advanced features that will be allowed. For example, if you specify CURSOR THRESHOLD, QUERY WAIT, those advanced features will be allowed—any other advanced features that occur in the code will cause the workflow to fail. The default is to check all of the normal advanced features.
Run Flag	Y	optional	Flag to indicate whether the workflow should run this check. Valid values are Y (run the check) or N (do not run the check).

Additional Input Parameters Defined in this Step: Check SQL Database Commands

Parameter Name	Default Value	Required	Description
Run Flag	Y	optional	Flag to indicate whether the workflow should run this check. Valid values are Y (run the check) or N (do not run the check).
SQL Commands	shutdown, sp_configure, create database, drop database, create login, create user, drop login, drop user, sp_grantdbaccess, sp_addlogin, sp_droplogin	optional	Comma-separated list of SQL commands that are not allowed. The default shows an example of how to fill out the list. You may want to customize this list for your configuration.

Additional Input Parameters Defined in this Step: Check SQL Database Links

Parameter Name	Default Value	Required	Description
Run Flag	Y	optional	Flag to indicate whether the workflow should run this check. Valid values are Y (run the check) or N (do not run the check).

Additional Input Parameters Defined in this Step: Check SQL Syntax

Parameter Name	Default Value	Required	Description
Run Flag	Y	optional	Flag to indicate whether the workflow should run this check. Valid values are Y (run the check) or N (do not run the check).

Additional Input Parameters Defined in this Step: Check SQL System Grants

Parameter Name	Default Value	Required	Description
Exception List	grant db_owner, grant ddladmin, grant sysadmin, grant securityadmin, grant serveradmin, grant processadmin, grant diskadmin, grant dbcreator	optional	Comma-separated list of SQL system privileges that will be allowed. For example, if you specify , those system privileges will be allowed—any other system privileges that occur in the code will cause the workflow to fail. The default shows an example of how to fill out the list. You may want to customize this list for your configuration.
Run Flag	Y	optional	Flag to indicate whether the workflow should run this

Additional Input Parameters Defined in this Step: Check SQL System Grants, continued

Parameter Name	Default Value	Required	Description
			check. Valid values are Y (run the check) or N (do not run the check).

Additional Input Parameters Defined in this Step: Match Regular Expression to SQL Server Scripts

Parameter Name	Default Value	Required	Description
Regular Expression		optional	The regular expression to be searched for in all of the SQL scripts to be deployed. If the specified regular expression is found, the workflow exits with a failure. For example: drop\s+table will match all statements that drop a table.
Run Flag	Y	optional	Flag to indicate whether the workflow should run this check. Valid values are Y (run the check) or N (do not run the check).

Additional Input Parameters Defined in this Step: Run SQL Server Script

Parameter Name	Default Value	Required	Description
Database Name	master	optional	The name of the database to which the specified SQL scripts will be applied.
Run Flag	Y	optional	Flag to indicate whether the workflow should run the SQL Server script. Valid values are Y (run the check) or N (do not run the check).

MS SQL Drop Database v2

This workflow is supported on the Windows operating system platform. The MS SQL Drop Database enables you to remove the target database from the MS SQL instance and from the DMA environment..

To use this workflow in your environment, see the following information:

Topic	Information Included
"Prerequisites for this Workflow" on the next page	List of prerequisites that must be satisfied before you can run this workflow
"How this Workflow Works" on page 650	Information about what the workflow does, including validation checks performed, steps executed, and step descriptions
"How to Run this Workflow" on page 651	Instructions for running this workflow in your environment
"Parameters for MS SQL - Drop Database" on page 653	List of input parameters for this workflow

Prerequisites for this Workflow

Be sure that the following prerequisites are satisfied before you run the MS SQL Drop Database workflow:

- This solution requires DMA version 10.30 (or later).

The latest DMA solution packs require the latest DMA platform. To use the latest solution packs, update the DMA platform. DMA10.50.001.000 solution packs are supported on DMA10.50.001.000 (and later).

- You have installed the Database Compliance solution pack.

The workflow must be able to:

- MS SQL service should be up and running.
- Log in to the MS SQL instance using MS SQL login credentials.
- It should drop the database upon connecting to the MS SQL instance.

The information presented here assumes the following: show assumptions

- DMA is installed and operational.
- At least one suitable target server is available.
- You are logged in to the DMA web interface.
- You have permission to create, edit, and deploy copies of the workflows included in this solution pack.

For more information about prerequisites for MS SQL database, refer to the [MS SQL Server Documentation](#).

How this Workflow Works

This workflow performs the following actions:

Drops a MS SQL database and removes it from the DMA environment.

Steps Executed by the Workflow

The MS SQL Drop Database workflow includes the following steps. Each step must complete successfully before the next step can start. If a step fails, the workflow reports a failure and all subsequent steps are skipped.

Steps Used by MS SQL

Workflow Step	Description
Gather Advanced Parameters for MS SQL Drop Database	This step gathers the parameters required to drop an MS SQL database.
MS SQL Check Database Exists	This step validates the existence of the database. Access to the master database is required for validation.
MS SQL Kill Processes	This step kills all the currently running user processes on the target database.
MS SQL Drop Database	This step drops the target database. To run this step, ensure that there are no active connections prior to running this step by running the "MS SQL: Kill Processes" step.
MS SQL Check Database Exists	This step validates the existence of a database. Access to the master database is required for validation.
Remove Database from Environment V2	This step removes the database from the DMA environment. This step takes the Instance Name and Database Name as input parameters. If the Instance Name and Database Name are not provided as input parameters, then the database against which the workflow is being executed will be removed from the DMA environment.

Note: For input parameter descriptions and defaults, see ["Parameters for MS SQL - Drop Database" on page 653](#).

How to Run this Workflow

The following instructions show you how to customize and run the MS SQL Drop Database workflow in your environment.

The workflow provides default values for some parameters. These default values are usually sufficient for a "typical" installation. You can override the defaults by specifying parameter values in the deployment. You can also expose additional parameters in the workflow, if necessary, to accomplish more advanced scenarios. Any parameters not explicitly specified in the deployment will have the default values listed in ["Parameters for MS SQL - Drop Database" on page 653](#).

Note: Before following this procedure, review the ["Prerequisites for this Workflow" on page 649](#), and ensure that all requirements are satisfied.

To use the Run MySQL Drop Database workflow:

1. Create a deployable copy of the workflow.
2. Determine the values that you will specify for the following parameters:

Note: There are no mandatory parameters required to run this workflow. All parameters are optional. You may need to expose additional parameters depending on your objectives.

See ["Parameters for MS SQL - Drop Database" on page 653](#) for detailed descriptions of all input parameters for this workflow, including default values.

3. In the workflow editor, expose any additional parameters that you need. You will specify values for those parameters when you create the deployment or at runtime.
4. Save the changes to the workflow (click **Save** in the lower right corner).
5. Create a new deployment.
6. On the Parameters tab, specify values (or set the type to Runtime Value) for the required parameters listed in step 2 and any additional parameters that you have exposed. You do not need to specify values for those parameters whose default values are appropriate for your environment.
7. On the Targets tab, specify one or more targets for this deployment.
8. Save the deployment (click **Save** in the lower right corner).
9. Run the workflow using this deployment, specifying any runtime parameters.

To verify the results:

The workflow will complete and report SUCCESS on the Console if it has run successfully. If an error occurs during workflow execution, the error is logged, and the workflow terminates in the FAILURE state. Also verify by checking that the target database no longer appears in the DMA Environment section.

Parameters for MS SQL - Drop Database

There are no mandatory parameters required to run this workflow. All parameters are optional. These parameters are not initially visible in a deployment. For these parameters, if you do not specify a value for a parameter, a default value is assigned.

MS SQL - Upgrade Standalone SQL Instance

This workflow is supported on the Windows operating system platform. The MS SQL - Upgrade Standalone SQL Instance enables you to update and existing instance of SQL Server.

To use this workflow in your environment, see the following information:

Topic	Information Included
"Prerequisites for this Workflow" on the next page	List of prerequisites that must be satisfied before you can run this workflow
"How this Workflow Works" on page 655	Information about what the workflow does, including validation checks performed, steps executed, and step descriptions
"How to Run this Workflow" on page 657	Instructions for running this workflow in your environment
"Parameters for MS SQL - Upgrade Standalone SQL Instance" on page 659	List of input parameters for this workflow

Prerequisites for this Workflow

Be sure that the following prerequisites are satisfied before you run the MS SQL - Upgrade Standalone SQL Instance workflow:

- This solution requires DMA version 10.30 (or later).

The latest DMA solution packs require the latest DMA platform. To use the latest solution packs, update the DMA platform. DMA10.50.001.000 solution packs are supported on DMA10.50.001.000 (and later).

- You have installed the Database Compliance solution pack.

The workflow must be able to:

- MS SQL service should be up and running.
- Log in to the MS SQL instance using MS SQL login credentials.
- It should drop the database upon connecting to the MS SQL instance.

The information presented here assumes the following: show assumptions

- DMA is installed and operational.
- At least one suitable target server is available.
- You are logged in to the DMA web interface.
- You have permission to create, edit, and deploy copies of the workflows included in this solution pack.

For more information about prerequisites for MS SQL database, refer to the [MS SQL Server Documentation](#).

How this Workflow Works

This workflow performs the following actions:

Upgrades an existing standalone instance of SQL Server 2005/08/08R2/12 to SQL Server 2008/08R2/12/14 on an existing Windows 2008/08R2/12/12 R2 server.

Steps Executed by the Workflow

The MS SQL - Upgrade Standalone SQL Instance workflow includes the following steps. Each step must complete successfully before the next step can start. If a step fails, the workflow reports a failure and all subsequent steps are skipped.

Steps Used by MS SQL

Workflow Step	Description
MS SQL - Parameters - Upgrade Standalone	This step gathers all the required parameters for a standalone SQL Server upgrade.
MS SQL - Advanced Parameters - Upgrade Standalone	This step gathers all the optional parameters for a standalone SQL Server upgrade. All advanced parameters are hidden in the deployment screen by default. In order to activate an advanced parameter, go into the Workflow, and change the parameter mapping from on this step from Blank to User Input.
Check If Download File Exists	This step is designed to facilitate the complicated methodologies that various companies use to distribute their software bundles for installation.
MS SQL - Create Install or Upgrade Template	This step verifies that all required parameters are provided, and writes any optional parameters to the template file if they are non-blank.
Unzip Archive	This step is to unzip a zip archive, verify if the input file exists, ensure the output directory exists, creates required directories, and deploys archived files.
MS SQL - Simulate - Install or Upgrade	This step verifies that all required parameters are provided, and the system meets minimum requirements.
MS SQL - Install or Upgrade	This step installs SQL Server 2008 by running the setup.exe program located on the installation media.
MS SQL Verify SQL Installation	This step determines if the target instance name of SQL Server is currently installed.
Windows Check for Pending Reboot	This step checks for any pending reboots.

Steps Used by MS SQL , continued

Workflow Step	Description
Discover SQL Databases	This step audits the server's physical environment looking for SQLServer instances and databases.
Windows Restart Server	This step restarts a system.
Windows Wait for Restart	This step is to wait 8 minutes for Windows server to finish restart.
MS SQL - Install or Upgrade	This installs SL Server 2008 by running the setup.exe program located on the installation media.
MS SQL Verify SQL Installation	This step determines if the target instance name of SQL Server is currently installed.

Note: For input parameter descriptions and defaults, see ["Parameters for MS SQL - Upgrade Standalone SQL Instance" on page 659.](#)

How to Run this Workflow

The following instructions show you how to customize and run the MS SQL Upgrade Standalone SQL Instance workflow in your environment.

The workflow provides default values for some parameters. These default values are usually sufficient for a "typical" installation. You can override the defaults by specifying parameter values in the deployment. You can also expose additional parameters in the workflow, if necessary, to accomplish more advanced scenarios. Any parameters not explicitly specified in the deployment will have the default values listed in ["Parameters for MS SQL - Upgrade Standalone SQL Instance" on page 659](#).

Note: Before following this procedure, review the ["Prerequisites for this Workflow" on page 654](#), and ensure that all requirements are satisfied.

To use the Run MS SQL - Upgrade Standalone SQL Instance workflow:

1. Create a deployable copy of the workflow.
2. Determine the values that you will specify for the following parameters:

Note: There are no mandatory parameters required to run this workflow. All parameters are optional. You may need to expose additional parameters depending on your objectives.

See ["Parameters for MS SQL - Upgrade Standalone SQL Instance" on page 659](#) for detailed descriptions of all input parameters for this workflow, including default values.
3. In the workflow editor, expose any additional parameters that you need. You will specify values for those parameters when you create the deployment or at runtime.
4. Save the changes to the workflow (click **Save** in the lower right corner).
5. Create a new deployment.
6. On the Parameters tab, specify values (or set the type to Runtime Value) for the required parameters listed in step 2 and any additional parameters that you have exposed. You do not need to specify values for those parameters whose default values are appropriate for your environment.
7. On the Targets tab, specify one or more targets for this deployment.
8. Save the deployment (click **Save** in the lower right corner).
9. Run the workflow using this deployment, specifying any runtime parameters.

To verify the results:

The workflow will complete and report SUCCESS on the Console if it has run successfully. If an error occurs during workflow execution, the error is logged, and the workflow terminates in the FAILURE state. Also verify by checking that the target database no longer appears in the DMA Environment section.

Parameters for MS SQL - Upgrade Standalone SQL Instance

The following tables describe the required and optional input parameters for this workflow. Some of these parameters may not be initially visible in a deployment. For some parameters, if you do not specify a value for a parameter, a default value is assigned.

Note: Only those parameters that are configurable in a standard deployment are listed here. Input parameters that must be mapped to output parameters of previous steps are not listed.

Parameters Defined in this Step: MS SQL - Parameters - Upgrade Standalone

Parameter Name	Default Value	Required	Description
Download From Software Directory	no default	optional	The name of the ZIP file containing the SQL Server setup files
Download Target Destination	no default	required	The local directory where the SQL Setup files should be stored.
Instance Name	MSSQLSERVER	required	The name of the newly created instance. Use MSSQLSERVER for the default instance, any other alphanumeric value for a named instance.

Additional Parameters Defined in this Step: MS SQL - Advanced Parameters - Upgrade Standalone

Parameter Name	Default Value	Required	Description
Additional Template Parameters	no default	optional	Pipe-delimited (" ") list of additional template parameters and values. SQMREPORTING 1 INSTANCEDIR "D:\SQLDirectory"
Installation Path	no default	optional	Specifies the location for the SQL Server program files.
Installer Account	no default	optional	The Windows account that will be performing the installation.
Installer Password	no default	optional	The password of the Windows account that will be performing the installation.
Product Key	no default	optional	Specifies the product key for the edition of SQL Server. If this parameter is not specified, Evaluation is used.
Skip Simulation	no default	optional	If set to "YES", workflow will skip Simulate step and proceed directly to install/upgrade step.

MS SQL Rollback Patch

This workflow is supported on the Windows operating system platform. The MS SQL Rollback Patch enables you to uninstall a SQL Server patch on a standalone 2005/2008/2008R2 instance.

To use this workflow in your environment, see the following information:

Topic	Information Included
"Prerequisites for this Workflow" on the next page	List of prerequisites that must be satisfied before you can run this workflow
"How this Workflow Works" on page 662	Information about what the workflow does, including validation checks performed, steps executed, and step descriptions
"How to Run this Workflow" on page 664	Instructions for running this workflow in your environment
"Parameters for MS SQL Rollback Patch" on page 666	List of input parameters for this workflow

Prerequisites for this Workflow

Be sure that the following prerequisites are satisfied before you run the MS SQL Rollback Patch workflow:

- This solution requires DMA version 10.30 (or later).

The latest DMA solution packs require the latest DMA platform. To use the latest solution packs, update the DMA platform. DMA10.50.001.000 solution packs are supported on DMA10.50.001.000 (and later).

- You have installed the Database Compliance solution pack.

The workflow must be able to:

- MS SQL service should be up and running.
- Log in to the MS SQL instance using MS SQL login credentials.
- It should drop the database upon connecting to the MS SQL instance.

The information presented here assumes the following: show assumptions

- DMA is installed and operational.
- At least one suitable target server is available.
- You are logged in to the DMA web interface.
- You have permission to create, edit, and deploy copies of the workflows included in this solution pack.

For more information about prerequisites for MS SQL database, refer to the [MS SQL Server Documentation](#).

How this Workflow Works

This workflow performs the following actions:

Uninstalls a SQL Server patch on a standalone 2005/2008/2008R2 instance. The default deployment will only show required parameters.

Steps Executed by the Workflow

The MS SQL Rollback Patch workflow includes the following steps. Each step must complete successfully before the next step can start. If a step fails, the workflow reports a failure and all subsequent steps are skipped.

Steps Used by MS SQL Rollback Patch

Workflow Step	Description
MS SQL Parameters Rollback Patch	This step gathers all the required parameters for a rollback (uninstall) of a SQL Server patch.
MS SQL Gather Advanced Parameters for Rollback Patch	This step gathers all the advanced parameters for a rollback (uninstall) of a SQL Server patch.
Windows Check for Pending Reboot	This step check for any pending reboots.
Check If Download File Exists	This step is designed to facilitate the complicated methodologies that various companies use to distribute their software bundles for installation.
MS SQL Verify Patch Rollback	This step verifies that a rollback of a Windows or SQL Server patch was successful.
Delete Directory	This step deletes a directory (folder).
Windows Restart Server	This step Restart a system
Download Software	This step automates the transfer of files from the HP SA Software Library to individual managed servers for use in downstream workflow steps.
MS SQL Rollback Patch	This step performs a rollback on a Windows or SQL Server patch.
Windows Wait for Restart	This step is to wait 8 minutes for Windows server to finish restart.
Unzip Archive	This step is to unzip a zip archive, verify if the input file exists, ensure the output directory exists, creates required directories, and deploys archived files.
MS SQL Verify Patch Rollback	This step verifies that a rollback of a Windows or SQL Server patch was successful.
Delete File	This step deletes the specified file.
Windows Check for Pending Reboot	This step checks for any pending reboots.

Steps Used by MS SQL Rollback Patch, continued

Workflow Step	Description
Delete Directory	This step deletes a directory (folder).
Windows Restart Server	This step restarts a system.
Discover SQL Databases	This step audits the server's physical environment looking for SQLServer instances and databases.
Windows Wait for Restart	This step is to wait 8 minutes for Windows server to finish restart.

Note: For input parameter descriptions and defaults, see "[Parameters for MS SQL Rollback Patch](#)" on page 666.

How to Run this Workflow

The following instructions show you how to customize and run the MS SQL Rollback Patch workflow in your environment.

The workflow provides default values for some parameters. These default values are usually sufficient for a "typical" installation. You can override the defaults by specifying parameter values in the deployment. You can also expose additional parameters in the workflow, if necessary, to accomplish more advanced scenarios. Any parameters not explicitly specified in the deployment will have the default values listed in ["Parameters for MS SQL Rollback Patch" on page 666](#).

Note: Before following this procedure, review the ["Prerequisites for this Workflow" on page 661](#), and ensure that all requirements are satisfied.

To use the Run MS SQL Rollback Patch workflow:

1. Create a deployable copy of the workflow.
2. Determine the values that you will specify for the following parameters:

Note: There are no mandatory parameters required to run this workflow. All parameters are optional. You may need to expose additional parameters depending on your objectives.

See ["Parameters for MS SQL Rollback Patch" on page 666](#) for detailed descriptions of all input parameters for this workflow, including default values.

3. In the workflow editor, expose any additional parameters that you need. You will specify values for those parameters when you create the deployment or at runtime.
4. Save the changes to the workflow (click **Save** in the lower right corner).
5. Create a new deployment.
6. On the Parameters tab, specify values (or set the type to Runtime Value) for the required parameters listed in step 2 and any additional parameters that you have exposed. You do not need to specify values for those parameters whose default values are appropriate for your environment.
7. On the Targets tab, specify one or more targets for this deployment.
8. Save the deployment (click **Save** in the lower right corner).
9. Run the workflow using this deployment, specifying any runtime parameters.

To verify the results:

The workflow will complete and report SUCCESS on the Console if it has run successfully. If an error occurs during workflow execution, the error is logged, and the workflow terminates in the FAILURE state. Also verify by checking that the target database no longer appears in the DMA Environment section.

Parameters for MS SQL Rollback Patch

The following tables describe the required and optional input parameters for this workflow. Some of these parameters may not be initially visible in a deployment. For some parameters, if you do not specify a value for a parameter, a default value is assigned.

Note: Only those parameters that are configurable in a standard deployment are listed here. Input parameters that must be mapped to output parameters of previous steps are not listed.

Input Parameters Defined in this Step: MS SQL Parameters Rollback Patch

Parameter Name	Default Value	Required	Description
Patch Name	no default	required	Name of the patch, the KB number of the patch, or "Latest Patch" to automatically rollback latest patch on instance. This field is case-insensitive.

MS SQL - Create AlwaysOn Availability Group v2

The MS SQL - Create AlwaysOn Availability Group workflow creates a new AlwaysOn Availability Group on the primary target, then adds secondary replicas to the group. Member databases will then be added to the Availability Group, while replica configuration is handled during the entire process.

To use this workflow in your environment, see the following information:

Topic	Information Included
"Prerequisites for this Workflow" on the next page	List of prerequisites that must be satisfied before you can run this workflow
"How this Workflow Works" on page 669	Information about what the workflow does, including validation checks performed, steps executed, and step descriptions
" How to Run this Workflow" on page 671	Instructions for running this workflow in your environment
"Parameters for MSSQL - Create AlwaysOn Availability Group" on page 673	List of input parameters for this workflow

Prerequisites for this Workflow

Be sure that the following prerequisites are satisfied before you run the MS SQL - Create AlwaysOn Availability Group workflow:

- This solution requires DMA version 10.50.001.000 (or later).

The latest DMA solution packs require the latest DMA platform. To use the latest solution packs, update the DMA platform. DMA10.50.001.000 solution packs are supported on DMA10.50.001.000 (and later).

- You have installed the Database Provisioning solution pack.
- An existing SQL server instance to be used as the target instance.
- Workflow needs to run against nodes that are members of the same Windows cluster.
- Each workflow target should be a standalone instance that is installed on a cluster node.
- Workflow should run under a domain account that has access to all instances to be added to new Availability Group, as well as has access to the Windows share where backup files will be saved.

The information presented here assumes the following: show assumptions

- DMA is installed and operational.
- At least one suitable target server (database) is available.
- You are logged in to the DMA web interface.
- You have permission to create, edit, and deploy copies of the workflows included in this solution pack.

For more information about prerequisites for MySQL database, refer to the [Microsoft SQL Server Documentation](#).

How this Workflow Works

This workflow performs the following actions:

- Creates a new AlwaysOn Availability Group on the primary target, then adds secondary replicas to the group.

Steps Executed by the Workflow

The MS SQL - Create AlwaysOn Availability Group workflow includes the following steps. Each step must complete successfully before the next step can start. If a step fails, the workflow reports a failure and all subsequent steps are skipped.

Steps Used by MS SQL - Create AlwaysOn Availability Group

Workflow Step	Description
MS SQL - Gather Parameters for AlwaysOn Group v2	This step gathers parameters to create AlwaysOn availability group.
MS SQL - Gather Advanced Parameters for AlwaysOn Group	This steps gathers advanced parameters to create AlwaysOn availability group.
MS SQL - Check AlwaysOn Prerequisites	This step checks for pre-requisites that are mandatory to create AlwaysOn group if the Windows version is greater than 2008, the installed SQL server is an Enterprise edition, and the server that if the AlwaysOn group is not a domain controller.
MS SQL - Enable AlwaysOn	This step enables the AlwaysOn feature on the instance that will be added to the AlwaysOn group.
MS SQL - Create Mirroring Endpoint v2	This step creates the endpoint and grants connect permission to the created endpoint.
MS SQL - Run Setup AlwaysOn Secondary v2	This step triggers the execution of subflow MS SQL - Setup AlwaysOn Secondary on the secondary servers.
MS SQL - Backup Databases for AlwaysOn	This step creates backup databases on an instance (Full, Differential, or Log backup types). The list of databases to backup can range from all databases (default), all except a select few (ignore list), or just a select few (exclusive list).
MS SQL - Create AlwaysOn Group	This step creates the AlwaysOn group.
MS SQL - Backup Databases for AlwaysOn	This step creates backup databases on an instance (Full, Differential, or Log backup types). The list of databases to backup can range from all databases (default), all except a select few (ignore list), or just a select few (exclusive list).
MS SQL - Run Join Secondary to AlwaysOn Group	This step triggers the subflow MS SQL - Join Secondary to AlwaysOn Group that in turn adds the secondary server to the AlwaysOn group.

Steps Used by MS SQL - Create AlwaysOn Availability Group, continued

Workflow Step	Description
MS SQL - Validate AlwaysOn Availability Group	This step validates, if the AlwaysOn group has been created appropriately.

How to Run this Workflow

The following instructions show you how to customize and run the MS SQL - Create AlwaysOn Availability Group workflow in your environment.

The workflow provides default values for some parameters. These default values are usually sufficient for a "typical" installation. You can override the defaults by specifying parameter values in the deployment. You can also expose additional parameters in the workflow, if necessary, to accomplish more advanced scenarios. Any parameters not explicitly specified in the deployment will have the default values listed in ["Parameters for MSSQL - Create AlwaysOn Availability Group" on page 673](#).

Note: Before following this procedure, review the ["Prerequisites for this Workflow" on page 668](#), and ensure that all requirements are satisfied.

To use the MS SQL - Create AlwaysOn Availability Group workflow:

1. Create a deployable copy of the workflow.
2. Determine the values that you will specify for the parameters.

Note: There are no mandatory parameters required to run this workflow. All parameters are optional. You may need to expose additional parameters depending on your objectives.
3. In the workflow editor, expose any additional parameters that you need. You will specify values for those parameters when you create the deployment or at runtime.
4. Save the changes to the workflow (click **Save** in the lower right corner).
5. Create a new deployment.
6. On the Parameters tab, specify values (or set the type to Run time Value) for the required parameters listed in step 2 and any additional parameters that you have exposed. You do not need to specify values for those parameters whose default values are appropriate for your environment.
7. On the Targets tab, specify one or more targets for this deployment.
8. Save the deployment (click **Save** in the lower right corner).
9. Run the workflow using this deployment, specifying any runtime parameters.

To verify the results:

The workflow will complete and report SUCCESS on the Console if it has run successfully. If an error occurs during workflow execution, the error is logged, and the workflow terminates in the FAILURE state. The database will be removed from the DMA environment section upon SUCCESS as well.

Use SQL Server Management Studio to verify that Availability Group has been created (see <http://msdn.microsoft.com/en-us/library/ff878267.aspx> for more information).

.

Parameters for MSSQL - Create AlwaysOn Availability Group

The following tables describe the required and optional input parameters for this workflow. Some of these parameters are not initially visible in a deployment. For most parameters, if you do not specify a value for a parameter, a default value is assigned.

Parameters Defined in this Step: MS SQL - Gather Parameters for AlwaysOn Group

Parameter Name	Default Value	Required	Description
Availability Group Name	no default	required	Specifies the name of the new Availability Group. It must be unique across all Availability Groups in the Windows cluster.
Databases in Group	no default	required	Comma-separated list of database names to be included in Availability Group.
List of Secondary Server-Instances	no default	required	Comma-separated list of server-instances to be secondaries. For example: Server1\Instance1,Server2\Instance2,Server3\Instance3.
Mirroring Endpoint Name	no default	required	Name of the endpoint that will be used for database mirroring,
Mirroring Endpoint Port	4022	required	Specifies the port number listened to for connections by the service broker TCP/IP protocol. Default is 4022. Valid values are between 1024 and 32767.
Path to Share for Backup Files	no default	required	A Windows share location that all the cluster nodes can access, which will store backup files for the group databases.
Primary Availability Mode	SYNCHRONOUS	required	Specifies whether the primary replica has to wait for the secondary replica to acknowledge the hardening (writing) of the log records to disk before the primary replica can commit the transaction on a given primary database. Valid values are SYNCHRONOUS and ASYNCHRONOUS.
Primary Failover Mode	AUTOMATIC	required	Specifies the failover mode of the primary instance. Valid values are AUTOMATIC and MANUAL.
Secondary Availability Modes	SYNCHRONOUS	required	Comma-separated list of availability modes of secondary instances. Including the primary instance, you can specify up to three instances with SYNCHRONOUS mode, while up to five can be specified with ASYNCHRONOUS mode.
Secondary Failover Modes	AUTOMATIC	required	Comma-separated list of Failover Modes of secondary instances. Including the primary instance, you can specify up to two instances with AUTOMATIC mode, while up there is no limit on instances with MANUAL mode.

Parameters Defined in this Step: MS SQL - Gather Advanced Parameters for AlwaysOn Group

Parameter Name	Default Value	Required	Description
Instance Password	no default	optional	Password for the instance that will be added to AlwaysOn group.
Instance User	no default	optional	User account to access the instance that will be added to AlwaysOn group.
List of Server-Instances	no default	optional	Comma-separated list of server-instances to be secondaries. For example: Server1\Instance1,Server2\Instance2,Server3\Instance3.
Primary Port Number	4022	optional	Specifies the port number listened to for connections by the service broker TCP/IP protocol. Default is 4022. Valid values are between 1024 and 32767.
Secondary Port Numbers	no default	optional	Comma-separated list of port numbers that will be used on the secondary server.
Subflow Parallel Execution	yes	optional	Value to represent whether all the secondary can be joined to the primary in parallel. Default is yes. Valid values are true, false, yes, and no.
Web API - Password	no default	optional	DMA user account password.
Web API - URL	no default	optional	DMA server URL.
Web API - Username	no default	optional	DMA user account.

MS SQL - Install Clustered SQL Instance v2

This workflow installs a new standalone instance of SQL Server 2008/2008 R2/2012/2014 on an already existing Windows 2003/2008/2008 R2/2012/2012 R2 server. The default deployment will only show required parameters.

To use this workflow in your environment, see the following information:

Topic	Information Included
Prerequisites	List of prerequisites that must be satisfied before you can run this workflow
How this workflow works	Information about what the workflow does, including validation checks performed, steps executed, and step descriptions
How to run this workflow	Instructions for running this workflow in your environment
Parameters for MS SQL - Install Standalone SQL Instance	List of input parameters for this workflow

Prerequisites

Before performing the procedures in this section, your environment must meet the following minimum requirements:

- An existing Windows 2008, 2008 R2, or 2012 cluster
- Installation software:

The SQL Server 2008, 2008 R2, or 2012 software installation files, obtained from Microsoft.

The installation media must be available locally or available for download from the software repository.

- Storage:

An available shared disk for SQL Server shared files

A staging directory with 4 gigabytes available to unzip the SQL Server software

- Permissions to create an SQL Server database:

System Stored Procedures (SP)

CREATE LOGIN

If using a non-default database owner, the `sp_changedbowner` process is available

If a non-default database owner is specified and does not exist, permission to create the appropriate login

- .NET 3.5 is installed.

Note: For additional information, see the "Run workflows as a Windows domain user" topic in the *DMA Administration Guide*.

- Licenses for SQL Server and DMA.

For additional requirements, see the following Microsoft documentation:

SQL Server version	Microsoft documentation
2008	Hardware and Software Requirements for Installing SQL Server 2008
2008 R2	Hardware and Software Requirements for Installing SQL Server 2008 R2
2012	Hardware and Software Requirements for Installing SQL Server 2012

How this workflow works

This workflow performs the following actions:

Installs a new clustered instance of SQL Server 2008, 2008 R2, 2012, or 2014 on an already existing Windows 2008/2008 R2/2012/2012 R2 cluster.

Steps Executed

The MS SQL - Install Clustered SQL Instance workflow includes the following steps. Each step must complete successfully before the next step can start. If a step fails, the workflow reports a failure and all subsequent steps are skipped.

Steps used by MS SQL - Install Clustered SQL Instance

Workflow Step	Description
MS SQL - Gather Parameters For Install Clustered SQL Instance	This step gathers all the required parameters for a clustered SQL 2008 install.
MS SQL - Gather Advanced Parameters For Install Clustered SQL Instance	This step gathers all the optional parameters for a clustered SQL 2008 install.
Check If Download File Exists	This step is designed to facilitate the complicated methodologies that various companies use to distribute their software bundles for installation.
MS SQL - Create Install or Upgrade Template	This step verifies that all required parameters are provided, and writes any optional parameters to the template file if they are non-blank.
Download Software	This step automates the transfer of files from the HP SA Software Library to individual managed servers for use in downstream workflow steps. Verifies checksum of each file transferred.
Unzip Archive	This step unzips a "zip" archive, verifies that the input file exists, ensures that output directory exists, creates required directories, and deploys archived files.
Delete File	This step verifies a specified file exists and deletes it.
MS SQL - Simulate - Install or Upgrade	This step verifies that all required parameters are provided, and the system meets minimum requirements.
Delete File	This step verifies a specified file exists and deletes it.
MS SQL - Install or Upgrade v2	This step installs SQL Server 2008 by running the setup.exe program located on the installation media.
MS SQL Verify SQL Installation	This step determines if the target instance name of SQL Server is currently installed.
Delete Directory	This directory verifies a specified file exists and deletes it.
Delete File	This step verifies a specified file exists and deletes it.

Steps used by MS SQL - Install Clustered SQL Instance, continued

Workflow Step	Description
Windows Check for Pending Reboot	Check for any pending reboots. This ensures that an installation can be run without a prior reboot requirement.
Discover SQL Databases	Audits the server's physical environment looking for SQLServer instances and databases.
Windows Restart Server	Restarts a system Input Wait Time: The number of seconds to wait before the reboot.
Delete File	This step verifies a specified file exists and deletes it.
Windows Check for Pending Reboot	Checks for any pending reboots. This ensures that an installation can be run without a prior reboot requirement.
Windows Wait for Restart	Waits 8 minutes for Windows server to finish restart.
Windows Restart Server	Restarts a system Input Wait Time: The number of seconds to wait before the reboot.
MS SQL - Install or Upgrade v2	This step installs SQL Server 2008 by running the setup.exe program located on the installation media.
Windows Wait for Restart	Waits 8 minutes for Windows server to finish restart.
MS SQL Verify SQL Installation	This step determines if the target instance name of SQL Server is currently installed.

How to run this workflow

The following instructions show you how to customize and run the MS SQL - Install Standalone SQL Instance workflow in your environment.

The workflow provides default values for some parameters. These default values are usually sufficient for a "typical" installation. You can override the defaults by specifying parameter values in the deployment. You can also expose additional parameters in the workflow, if necessary, to accomplish more advanced scenarios. Any parameters not explicitly specified in the deployment will have the default values listed in [Parameters for MS SQL - Install Standalone SQL Instance](#).

Note: Before following this procedure, review the [Prerequisites](#), and ensure that all requirements are satisfied.

To use the MS SQL - Install Standalone SQL Instance workflow:

1. Create a deployable copy of the workflow.

Determine the values that you will specify for the following parameters.

The following tables describe the required and optional input parameters for this workflow.

Step: MS SQL - Gather Parameters For Install Clustered SQL Instance

Parameter	Required	Example Value	Description
Cluster Administrator Account	required	Win12\Administrator	The Windows domain user that will run the setup operation. This user requires elevated administrator privileges on the cluster. Format: <DOMAIN>\<USERNAME>
Cluster Administrator Password	required	●●●	Password for the Windows domain user that will run the setup operation. This user requires elevated administrator privileges on the cluster. Must be a strong Windows password.
Download From Software Directory	optional	SQL12.zip	The name of the ZIP file that contains the SQL Server installation software files obtained from Microsoft. Note: If necessary, manually zip the installation software files up.
Download Target Destination	required	C:\temp	The local directory where the SQL Server setup files are stored: If source files are in the software repository: Location where Download From Software Directory will be downloaded and extracted If source files are on the target: Location where the Microsoft SQL Server installation files already exist—not zipped up Upon a successful workflow completion, all downloaded and extracted files are cleaned up.
Instance Name	required	SQL-CLUSTER\InstanceA	The name of the newly created virtual server and instance. Format: <Virtual Server>\<Instance Name> Use MSSQLSERVER for the default instance and any other alphanumeric value for a named instance.
Public IP Address	required	DHCP	Public IP Address.

Step: MS SQL - Gather Parameters For Install Clustered SQL Instance, continued

Parameter	Required	Example Value	Description
			For SQL Server 2012 set to DHCP.
Public IP Network Name	required		IP Network Name for the clusters. Format: <Network Name>:<Subnet Mask> For example: Public:255.255.255.0
SQL Agent Account	required	Win12\Administrator	The login account for the SQL Server Agent service. Can be a local Windows user, a domain user, or a built-in account (for example: NT AUTHORITY\NETWORK SERVICE). If not a built-in account, also specify SQL Agent Password. This parameter is optional for SQL Server 2008 or 2008 R2.
SQL Agent Password	required	●●●	Specify if SQL Agent Account is specified. This parameter is optional for SQL Server 2008 or 2008 R2.
SQL Service Account	required	Win12\Administrator	The login account for the SQL service. Can be a local Windows user, a domain user, or a built-in account (for example: NT AUTHORITY\NETWORK SERVICE). If not a built-in account, also specify SQL Service Password. This parameter is optional for SQL Server 2008 or 2008 R2.
SQL Service Password	required	●●●	Specify if SQL Service Account is specified. This parameter is optional for SQL Server 2008 or 2008 R2.
SQL Sysadmin Accounts	required	Win12\Administrator	A comma-delimited list of user accounts that will be set as system administrators. Each account must either be a local Windows user or a domain user. This parameter is optional for SQL Server 2008 or 2008 R2.

Step: MS SQL - Gather Advanced Parameters For Install Clustered SQL Instance

Parameter	Required	Example Value	Description
Additional Template Parameters	optional	SQMREPORTING 1 INSTANCEDIR "D:\SQLDirectory"	Pipe-delimited () list of additional template parameters and values. Should follow this example: SQMREPORTING 1 INSTANCEDIR "D:\SQLDirectory"
Backup Directory		?	Specifies the directory for backup files.
Cluster Node Names	optional	?	Comma-delimited list of node members' hostnames, including target hostname. Acceptable format: [Node1Hostname], [Node2Hostname]
Data File Location	optional	?	The location for the SQL Server program files.
Database Data Directory		?	Specifies the directory for the data files for user databases.
Database Log Directory		?	Specifies the directory for the log files for user databases.
Failover Cluster Disks		SQL Data,SQL Log	Specifies the list of shared disks to be included in the SQL Server failover cluster resource group.
Install Components	optional	?	A comma-delimited list that specifies which components to install. Feature names are case sensitive. For a list of components for SQL Server 2008 R2 (as well as links to previous versions), see: msdn.microsoft.com/en-us/library/ms144259(v=SQL.105).aspx#Feature
Installation Path	optional	?	The location for the SQL Server program files.
Installer Account	optional	?	The Windows account that will perform the installation.
Installer Password	optional	?	The password of the Windows account that will perform the installation
Product Key	optional	?	Specifies the product key for the edition of SQL Server. If this

Step: MS SQL - Gather Advanced Parameters For Install Clustered SQL Instance, continued

Parameter	Required	Example Value	Description
			parameter is not specified, Evaluation is used.
SA Password	optional	?	The password for the SQL Server SA account. If specified, the security mode will be set to SQL authentication. If left blank, security mode will be set to Windows authentication.
SQL Agent Account	optional	Win12\Administrator	The login account for the SQL Server Agent service. Can be a local Windows user, a domain user, or a built-in account (for example, NT AUTHORITY\NETWORK SERVICE). If not a built-in account, also specify SQL Agent Password.
SQL Agent Domain Group	optional	?	The domain group that the SQL Agent Account user is a member of.
SQL Agent Password	optional	●●●	Specify if SQL Agent Account is specified.
SQL Browser Account	optional	?	The login account for the SQL Server Agent service. Can be a local Windows user, a domain user, or a built-in account (for example, NT AUTHORITY\NETWORK SERVICE). If not a built-in account, also specify SQL Browser Password.
SQL Browser Password	required	?	Required if SQL Browser Account is specified and is not a built-in account.
SQL Cluster Domain Group	optional	?	The domain group that the SQL Service Account user is a member of.
SQL Cluster Resource Group	optional	?	The name of the cluster resource group where the SQL cluster will be installed. This cluster group should already be created by a system administrator. The cluster resource group will have

Step: MS SQL - Gather Advanced Parameters For Install Clustered SQL Instance, continued

Parameter	Required	Example Value	Description
			the shared disks where the SQL data files and shared program files will be stored.
SQL Cluster Shared Directory	optional	?	The path to the directory where the shared cluster program files will be stored. Must be on a disk shared by all nodes of the cluster.
SQL Collation	optional	?	The collation of the instance. If left blank, the instance will be installed with the collation of the OS.
SQL Service Account	optional	Win12\Administrator	The login account for the SQL Server service. Can be a local Windows user, a domain user, or a built-in account (for example, NT AUTHORITY\NETWORK SERVICE). If not a built-in account, also specify SQL Service Password.
SQL Service Password	required	●●●	Required if SQL Service Account is specified and is not a built-in account.
SQL Sysadmin Accounts	required	Win12\Administrator	<p>Optional, only applies to SQL Server 2008 and 2008 R2 installs. Not applicable for SQL Server 2005. A comma-delimited list of user accounts that will be set as system administrators. Each account must either be a local Windows user or a domain user.</p> <p>A comma-delimited list of user accounts that will be set as system administrators.</p> <p>Each account must either be a local Windows user or a domain user.</p> <p>This parameter is optional for SQL Server 2008 or 2008 R2.</p>
Skip Simulation	optional		If set to "YES", workflow will skip Simulate step and proceed directly to install/upgrade step.
TempDB	NA	NA	Specifies the directory for the

Step: MS SQL - Gather Advanced Parameters For Install Clustered SQL Instance, continued

Parameter	Required	Example Value	Description
Data Directory			data files for tempdb.
TempDB Log Directory	NA	NA	Specifies the directory for the log files for tempdb.
Update Source	NA	MU	The location where SQL Server setup will obtain product updates. The valid values are "MU" to search Microsoft Update, a valid folder path, a relative path such as .\MyUpdates or a UNC share.

2. In the workflow editor, expose any additional parameters that you need. You will specify values for those parameters when you create the deployment or at runtime.
3. Save the changes to the workflow (click **Save** in the lower right corner).
4. Create a new deployment. See "Create a Deployment" in *DMA Quick Start Tutorial* for instructions.
5. On the Parameters tab, specify values (or set the type to Runtime Value) for the required parameters listed in step 2 and any additional parameters that you have exposed. You do not need to specify values for those parameters whose default values are appropriate for your environment.
6. On the Targets tab, specify one or more targets for this deployment.
7. Save the deployment (click **Save** in the lower right corner).
8. Run the workflow using this deployment, specifying any runtime parameters. See "Run Your Workflow" in (*DMA Quick Start Tutorial* for instructions.

To verify the results:

The workflow will complete and report SUCCESS on the Console if it has run successfully. If an error occurs during workflow execution, the error is logged, and the workflow terminates in the FAILURE state.

Parameters for MS SQL - Install Clustered SQL Instance

The following tables describe the required and optional input parameters for this workflow.

Step: MS SQL - Gather Parameters For Install Clustered SQL Instance

Parameter	Required	Example Value	Description
Cluster Administrator Account	required	Win12\Administrator	The Windows domain user that will run the setup operation. This user requires elevated administrator privileges on the cluster. Format: <DOMAIN>\<USERNAME>
Cluster Administrator Password	required	●●●	Password for the Windows domain user that will run the setup operation. This user requires elevated administrator privileges on the cluster. Must be a strong Windows password.
Download From Software Directory	optional	SQL12.zip	The name of the ZIP file that contains the SQL Server installation software files obtained from Microsoft. Note: If necessary, manually zip the installation software files up.
Download Target Destination	required	C:\temp	The local directory where the SQL Server setup files are stored: If source files are in the software repository: Location where Download From Software Directory will be downloaded and extracted If source files are on the target: Location where the Microsoft SQL Server installation files already exist—not zipped up Upon a successful workflow completion, all downloaded and extracted files are cleaned up.
Instance Name	required	SQL-CLUSTER\InstanceA	The name of the newly created virtual server and instance. Format: <Virtual Server>\<Instance Name> Use MSSQLSERVER for the default instance and any other alphanumeric value for a named instance.
Public IP Address	required	DHCP	Public IP Address. For SQL Server 2012 set to DHCP.
Public IP Network Name	required		IP Network Name for the clusters. Format: <Network Name>:<Subnet Mask> For example: Public:255.255.255.0
SQL Agent	required	Win12\Administrator	The login account for the SQL Server

Step: MS SQL - Gather Parameters For Install Clustered SQL Instance, continued

Parameter	Required	Example Value	Description
Account			<p>Agent service. Can be a local Windows user, a domain user, or a built-in account (for example: NT AUTHORITY\NETWORK SERVICE).</p> <p>If not a built-in account, also specify SQL Agent Password.</p> <p>This parameter is optional for SQL Server 2008 or 2008 R2.</p>
SQL Agent Password	required	●●●	<p>Specify if SQL Agent Account is specified.</p> <p>This parameter is optional for SQL Server 2008 or 2008 R2.</p>
SQL Service Account	required	Win12\Administrator	<p>The login account for the SQL service. Can be a local Windows user, a domain user, or a built-in account (for example: NT AUTHORITY\NETWORK SERVICE).</p> <p>If not a built-in account, also specify SQL Service Password.</p> <p>This parameter is optional for SQL Server 2008 or 2008 R2.</p>
SQL Service Password	required	●●●	<p>Specify if SQL Service Account is specified.</p> <p>This parameter is optional for SQL Server 2008 or 2008 R2.</p>
SQL Sysadmin Accounts	required	Win12\Administrator	<p>A comma-delimited list of user accounts that will be set as system administrators.</p> <p>Each account must either be a local Windows user or a domain user.</p> <p>This parameter is optional for SQL Server 2008 or 2008 R2.</p>

Step: MS SQL - Gather Advanced Parameters For Install Clustered SQL Instance

Parameter	Required	Example Value	Description
Additional Template Parameters	optional	SQMREPORTING 1 INSTANCEDIR "D:\SQLDirector y"	<p>Pipe-delimited () list of additional template parameters and values. Should follow this example: SQMREPORTING 1 INSTANCEDIR "D:\SQLDirector y"</p>
Backup		?	Specifies the directory for backup

Step: MS SQL - Gather Advanced Parameters For Install Clustered SQL Instance, continued

Parameter	Required	Example Value	Description
Directory			files.
Cluster Node Names	optional	?	Comma-delimited list of node members' hostnames, including target hostname. Acceptable format: [Node1Hostname], [Node2Hostname]
Data File Location	optional	?	The location for the SQL Server program files.
Database Data Directory		?	Specifies the directory for the data files for user databases.
Database Log Directory		?	Specifies the directory for the log files for user databases.
Failover Cluster Disks		SQL Data,SQL Log	Specifies the list of shared disks to be included in the SQL Server failover cluster resource group.
Install Components	optional	?	A comma-delimited list that specifies which components to install. Feature names are case sensitive. For a list of components for SQL Server 2008 R2 (as well as links to previous versions), see: msdn.microsoft.com/en-us/library/ms144259(v=SQL.105).aspx#Feature
Installation Path	optional	?	The location for the SQL Server program files.
Installer Account	optional	?	The Windows account that will perform the installation.
Installer Password	optional	?	The password of the Windows account that will perform the installation
Product Key	optional	?	Specifies the product key for the edition of SQL Server. If this parameter is not specified, Evaluation is used.
SA Password	optional	?	The password for the SQL Server SA account. If specified, the security mode will be set to SQL authentication. If left blank, security mode will be set to Windows authentication.
SQL Agent Account	optional	Win12\Administrator	The login account for the SQL Server Agent service. Can be a local Windows user, a domain

Step: MS SQL - Gather Advanced Parameters For Install Clustered SQL Instance, continued

Parameter	Required	Example Value	Description
			user, or a built-in account (for example, NT AUTHORITY\NETWORK SERVICE). If not a built-in account, also specify SQL Agent Password.
SQL Agent Domain Group	optional	?	The domain group that the SQL Agent Account user is a member of.
SQL Agent Password	optional	●●●	Specify if SQL Agent Account is specified.
SQL Browser Account	optional	?	The login account for the SQL Server Agent service. Can be a local Windows user, a domain user, or a built-in account (for example, NT AUTHORITY\NETWORK SERVICE). If not a built-in account, also specify SQL Browser Password.
SQL Browser Password	required	?	Required if SQL Browser Account is specified and is not a built-in account.
SQL Cluster Domain Group	optional	?	The domain group that the SQL Service Account user is a member of.
SQL Cluster Resource Group	optional	?	The name of the cluster resource group where the SQL cluster will be installed. This cluster group should already be created by a system administrator. The cluster resource group will have the shared disks where the SQL data files and shared program files will be stored.
SQL Cluster Shared Directory	optional	?	The path to the directory where the shared cluster program files will be stored. Must be on a disk shared by all nodes of the cluster.
SQL Collation	optional	?	The collation of the instance. If left blank, the instance will be installed with the collation of the OS.
SQL Service Account	optional	Win12\Administrator	The login account for the SQL Server service. Can be a local Windows user, a domain user, or a built-in account (for example, NT AUTHORITY\NETWORK SERVICE). If not a built-in account, also specify SQL Service Password.

Step: MS SQL - Gather Advanced Parameters For Install Clustered SQL Instance, continued

Parameter	Required	Example Value	Description
SQL Service Password	required	●●●	Required if SQL Service Account is specified and is not a built-in account.
SQL Sysadmin Accounts	required	Win12\Administrator	<p>Optional, only applies to SQL Server 2008 and 2008 R2 installs. Not applicable for SQL Server 2005. A comma-delimited list of user accounts that will be set as system administrators. Each account must either be a local Windows user or a domain user.</p> <p>A comma-delimited list of user accounts that will be set as system administrators.</p> <p>Each account must either be a local Windows user or a domain user.</p> <p>This parameter is optional for SQL Server 2008 or 2008 R2.</p>
Skip Simulation	optional		If set to "YES", workflow will skip Simulate step and proceed directly to install/upgrade step.
TempDB Data Directory	NA	NA	Specifies the directory for the data files for tempdb.
TempDB Log Directory	NA	NA	Specifies the directory for the log files for tempdb.
Update Source	NA	MU	The location where SQL Server setup will obtain product updates. The valid values are "MU" to search Microsoft Update, a valid folder path, a relative path such as .\MyUpdates or a UNC share.

MS SQL - Add Node to Cluster v3

This workflow installs a new clustered instance of SQL Server 2008, 2008 R2, 2012, or 2014 on an already existing Windows 2008/2008 R2/2012/2012 R2 cluster. The default deployment will only show required parameters.

To use this workflow in your environment, see the following information:

Topic	Information Included
"Prerequisites" below	List of prerequisites that must be satisfied before you can run this workflow
"How this workflow works" on the next page	Information about what the workflow does, including validation checks performed, steps executed, and step descriptions
"How to run this workflow" on page 692	Instructions for running this workflow in your environment
"Parameters for MS SQL - Add Node to Cluster" on page 696	List of input parameters for this workflow

Prerequisites

Before performing the procedures in this section, your environment must meet the following minimum requirements:

- An existing Windows 2008, 2008 R2, or 2012 cluster
- Installation software:

The SQL Server 2008, 2008 R2, or 2012 software installation files, obtained from Microsoft.

The installation media must be available locally or available for download from the software repository.

- Storage:

An available shared disk for SQL Server shared files

A staging directory with 4 gigabytes available to unzip the SQL Server software

- Permissions to create an SQL Server database:

System Stored Procedures (SP)

CREATE LOGIN

If using a non-default database owner, the `sp_changedbowner` process is available

If a non-default database owner is specified and does not exist, permission to create the appropriate login

- .NET 3.5 is installed.

Note: For additional information, see the "Run workflows as a Windows domain user" topic in the *DMA Administration Guide*.

- Licenses for SQL Server and DMA.

For additional requirements, see the following Microsoft documentation:

SQL Server version	Microsoft documentation
2008	Hardware and Software Requirements for Installing SQL Server 2008
2008 R2	Hardware and Software Requirements for Installing SQL Server 2008 R2
2012	Hardware and Software Requirements for Installing SQL Server 2012

How this workflow works

This workflow installs a new standalone instance of SQL Server 2008/2008 R2/2012/2014 on an already existing Windows 2003/2008/2008 R2/2012/2012 R2 server.

Steps Executed

The MS SQL - Add Node to Cluster workflow includes the following steps. Each step must complete successfully before the next step can start. If a step fails, the workflow reports a failure and all subsequent steps are skipped.

Steps used by MS SQL - Add Node to Cluster

Workflow Step	Description
MS SQL - Parameters - Add Node to Cluster	Gathers all the required parameters for a standalone SQL Server install.
MS SQL - Advanced Parameters - Add Node to Cluster V2	Gather all the optional parameters for a standalone SQL Server install
Check If Download File Exists	This step is designed to facilitate the complicated methodologies that various companies use to distribute their software bundles for installation.
MS SQL - Create Install or Upgrade Template	This step verifies that all required parameters are provided, and writes any optional parameters to the template file if they are non-blank.
Download Software	This step automates the transfer of files from the HP SA Software Library to individual managed servers for use in downstream workflow steps. Verifies checksum of each file transferred.
Unzip Archive	This step unzips a "zip" archive, verifies that the input file exists, ensures that output directory exists, creates required directories, and deploys archived files.
Delete File	This step verifies a specified file exists and deletes it.
MS SQL - Simulate - Install or Upgrade	This step verifies that all required parameters are provided, and the system meets minimum requirements.
Delete File	This step verifies a specified file exists and deletes it.
MS SQL - Install or Upgrade v2	This step installs SQL Server 2008 by running the setup.exe program located on the installation media.

Steps used by MS SQL - Add Node to Cluster, continued

Workflow Step	Description
MS SQL Verify SQL Installation	This step determines if the target instance name of SQL Server is currently installed.
Delete Directory	This directory verifies a specified file exists and deletes it.
Delete File	This step verifies a specified file exists and deletes it.
Windows Check for Pending Reboot	Check for any pending reboots. This ensures that an installation can be run without a prior reboot requirement.
Discover SQL Databases	Audits the server's physical environment looking for SQLServer instances and databases.
Windows Restart Server	Restarts a system Input Wait Time: The number of seconds to wait before the reboot.
Delete File	This step verifies a specified file exists and deletes it.
Windows Check for Pending Reboot	Checks for any pending reboots. This ensures that an installation can be run without a prior reboot requirement.
Windows Wait for Restart	Waits 8 minutes for Windows server to finish restart.
Windows Restart Server	Restarts a system Input Wait Time: The number of seconds to wait before the reboot.
MS SQL - Install or Upgrade v2	This step installs SQL Server 2008 by running the setup.exe program located on the installation media.
Windows Wait for Restart	Waits 8 minutes for Windows server to finish restart.
MS SQL Verify SQL Installation	This step determines if the target instance name of SQL Server is currently installed.

How to run this workflow

The following instructions show you how to customize and run the MS SQL - Add Node to Cluster workflow in your environment.

The workflow provides default values for some parameters. These default values are usually sufficient for a "typical" installation. You can override the defaults by specifying parameter values in the deployment. You can also expose additional parameters in the workflow, if necessary, to accomplish more advanced scenarios. Any parameters not explicitly specified in the deployment will have the default values listed in ["Parameters for MS SQL - Add Node to Cluster" on page 696](#).

Note: Before following this procedure, review the ["Prerequisites" on page 690](#), and ensure that all requirements are satisfied.

To use the MS SQL - Add Node to Cluster workflow:

1. Create a deployable copy of the workflow (see "Create a Deployable Workflow" in *DMA Quick Start Tutorial*)
 - a. Determine the values that you will specify for the following parameters.

The following tables describe the required and optional input parameters for this workflow.

Step: MS SQL - Parameters - Add Node to Cluster

Parameter	Description	Example Value
Cluster Administrator Account	Required: The Windows domain user that will run the setup operation. This user requires elevated administrator privileges on the cluster. Format: <DOMAIN>\<USERNAME>	Win12\Administrator
Cluster Administrator Password	Required: Password for the Windows domain user that will run the setup operation. This user requires elevated administrator privileges on the cluster. Must be a strong Windows password.	●●●
Download From Software Directory	Optional: The name of the ZIP file that contains the SQL Server installation software files obtained from Microsoft. Note: If necessary, manually zip the installation software files up.	SQL12.zip
Download Target Destination	Required: The local directory where the SQL Server setup files are stored: If source files are in the software repository: Location where Download From Software Directory will be downloaded and extracted If source files are on the target: Location where the Microsoft SQL Server installation files already exist—not zipped up Upon a successful workflow completion, all downloaded and extracted files are cleaned up.	C:\temp
Instance Name	Required: The name of the newly created virtual server and instance. Format: <Virtual Server>\<Instance Name>	SQL-CLUSTER\InstanceA

Step: MS SQL - Parameters - Add Node to Cluster, continued

Parameter	Description	Example Value
	Use MSSQLSERVER for the default instance and any other alphanumeric value for a named instance.	

Step: MS SQL - Advanced Parameters - Add Node to Cluster

Parameter	Description	Example Value
Additional Template Parameters	Optional: Pipe-delimited () list of additional template parameters and values. Should follow this example: SQMREPORTING 1 INSTANCEDIR "D:\SQLDirectory"	SQMREPORTING 1 INSTANCEDIR "D:\SQLDirectory"
Installer Account	Optional: The Windows account that will perform the installation.	?
Installer Password	Optional: The password of the Windows account that will perform the installation	?
Product Key	Optional: Specifies the product key for the edition of SQL Server. If this parameter is not specified, Evaluation is used.	?
SQL Agent Account	Optional: The login account for the SQL Server Agent service. Can be a local Windows user, a domain user, or a built-in account (for example, NT AUTHORITY\NETWORK SERVICE). If not a built-in account, also specify SQL Agent Password.	Win12\Administrator
SQL Agent Password	Optional: Specify if SQL Agent Account is specified.	●●●
SQL Service Account	Optional: The login account for the SQL Server service. Can be a local Windows user, a domain user, or a built-in account (for example, NT AUTHORITY\NETWORK SERVICE). If not a built-in account, also specify SQL Service Password.	Win12\Administrator
SQL Service Password	Required if SQL Service Account is specified and is not a built-in account.	●●●

Step: MS SQL - Advanced Parameters - Add Node to Cluster, continued

Parameter	Description	Example Value
Public IP Address	Required: Public IP Address. For SQL Server 2012 set to DHCP.	DHCP
Public IP Network Name	Required: IP Network Name for the clusters. Format: <Network Name>:<Subnet Mask> For example: Public:255.255.255.0	
SQL Agent Account	Required: The login account for the SQL Server Agent service. Can be a local Windows user, a domain user, or a built-in account (for example: NT AUTHORITY\NETWORK SERVICE). If not a built-in account, also specify SQL Agent Password. This parameter is optional for SQL Server 2008 or 2008 R2.	Win12\Administrator
SQL Agent Password	Required: Specify if SQL Agent Account is specified. This parameter is optional for SQL Server 2008 or 2008 R2.	●●●
SQL Service Account	Required: The login account for the SQL service. Can be a local Windows user, a domain user, or a built-in account (for example: NT AUTHORITY\NETWORK SERVICE). If not a built-in account, also specify SQL Service Password. This parameter is optional for SQL Server 2008 or 2008 R2.	Win12\Administrator
SQL Service Password	Required: Specify if SQL Service Account is specified. This parameter is optional for SQL Server 2008 or 2008 R2.	●●●
SQL Sysadmin Accounts	Required: A comma-delimited list of user accounts that will be set as system administrators. Each account must either be a local Windows user or a domain user.	Win12\Administrator

Step: MS SQL - Advanced Parameters - Add Node to Cluster, continued

Parameter	Description	Example Value
	This parameter is optional for SQL Server 2008 or 2008 R2.	
Skip Simulation	If set to "YES", workflow will skip Simulate step and proceed directly to install/upgrade step	NA

- In the workflow editor, expose any additional parameters that you need. You will specify values for those parameters when you create the deployment or at runtime.
- Save the changes to the workflow (click **Save** in the lower right corner).
- Create a new deployment. See "Create a Deployment" in *DMA Quick Start Tutorial* for instructions.
- On the Parameters tab, specify values (or set the type to Runtime Value) for the required parameters listed in step 2 and any additional parameters that you have exposed. You do not need to specify values for those parameters whose default values are appropriate for your environment.
- On the Targets tab, specify one or more targets for this deployment.
- Save the deployment (click **Save** in the lower right corner).
- Run the workflow using this deployment, specifying any runtime parameters. See "Run Your Workflow" in (*DMA Quick Start Tutorial* for instructions.

To verify the results:

The workflow will complete and report SUCCESS on the Console if it has run successfully. If an error occurs during workflow execution, the error is logged, and the workflow terminates in the FAILURE state.

Parameters for MS SQL - Add Node to Cluster

The following tables describe the required and optional input parameters for this workflow.

Step: MS SQL - Parameters - Add Node to Cluster

Parameter	Required	Example Value	Description
Cluster Administrator Account	required	Win12\Administrator	The Windows domain user that will run the setup operation. This user requires elevated administrator privileges on the cluster. Format: <DOMAIN>\<USERNAME>
Cluster Administrator	required	●●●	Password for the Windows domain user

Step: MS SQL - Parameters - Add Node to Cluster, continued

Parameter	Required	Example Value	Description
Password			that will run the setup operation. This user requires elevated administrator privileges on the cluster. Must be a strong Windows password.
Download From Software Directory	optional	SQL12.zip	<p>The name of the ZIP file that contains the SQL Server installation software files obtained from Microsoft.</p> <p>Note: If necessary, manually zip the installation software files up.</p>
Download Target Destination	required	C:\temp	<p>The local directory where the SQL Server setup files are stored:</p> <p>If source files are in the software repository: Location where Download From Software Directory will be downloaded and extracted</p> <p>If source files are on the target: Location where the Microsoft SQL Server installation files already exist—not zipped up</p> <p>Upon a successful workflow completion, all downloaded and extracted files are cleaned up.</p>
Instance Name	required	SQL-CLUSTER\InstanceA	<p>The name of the newly created virtual server and instance.</p> <p>Format: <Virtual Server>\<Instance Name></p> <p>Use MSSQLSERVER for the default instance and any other alphanumeric value for a named instance.</p>

Step: MS SQL - Advanced Parameters - Add Node to Cluster

Parameter	Required	Example Value	Description
Additional Template Parameters	optional	SQMREPORTING 1 INSTANCEDIR "D:\SQLDirectory"	Pipe-delimited () list of additional template parameters and values. Should follow this example: SQMREPORTING 1 INSTANCEDIR "D:\SQLDirectory"
Installer Account	optional	?	The Windows account that will perform the installation.
Installer Password	optional	?	The password of the Windows account that will perform the installation

Step: MS SQL - Advanced Parameters - Add Node to Cluster, continued

Parameter	Required	Example Value	Description
Product Key	optional	?	Specifies the product key for the edition of SQL Server. If this parameter is not specified, Evaluation is used.
Public IP Address	required	DHCP	Public IP Address. For SQL Server 2012 set to DHCP.
Public IP Network Name	required		IP Network Name for the clusters. Format: <Network Name>:<Subnet Mask> For example: Public:255.255.255.0
SQL Agent Account	optional	Win12\Administrator	The login account for the SQL Server Agent service. Can be a local Windows user, a domain user, or a built-in account (for example, NT AUTHORITY\NETWORK SERVICE). If not a built-in account, also specify SQL Agent Password.
SQL Agent Password	optional	●●●	Specify if SQL Agent Account is specified.
SQL Service Account	optional	Win12\Administrator	The login account for the SQL Server service. Can be a local Windows user, a domain user, or a built-in account (for example, NT AUTHORITY\NETWORK SERVICE). If not a built-in account, also specify SQL Service Password.
SQL Service Password	required	●●●	Required if SQL Service Account is specified and is not a built-in account.
Skip Simulation	optional	NA	If set to "YES", workflow will skip Simulate step and proceed directly to install/upgrade step

MS SQL - Create Database v2

This workflow creates a new database on the target instance. The only required parameter is "Database Name", but there are several optional parameters to customize the process.

To use this workflow in your environment, see the following information:

Topic	Information Included
"Prerequisites" below	List of prerequisites that must be satisfied before you can run this workflow
"How this workflow works" on the next page	Information about what the workflow does, including validation checks performed, steps executed, and step descriptions
"How to run this workflow" on page 701	Instructions for running this workflow in your environment
"Parameters for MS SQL - Create Database" on page 703	List of input parameters for this workflow

Prerequisites

Before performing the procedures in this section, your environment must meet the following minimum requirements:

- An existing Windows 2008, 2008 R2, or 2012 cluster
- Installation software:

The SQL Server 2008, 2008 R2, or 2012 software installation files, obtained from Microsoft.

The installation media must be available locally or available for download from the software repository.

- Storage:

An available shared disk for SQL Server shared files

A staging directory with 4 gigabytes available to unzip the SQL Server software

- Permissions to create an SQL Server database:

System Stored Procedures (SP)

CREATE LOGIN

If using a non-default database owner, the `sp_changedbowner` process is available

If a non-default database owner is specified and does not exist, permission to create the appropriate login

- .NET 3.5 is installed.

Note: For additional information, see the "Run workflows as a Windows domain user" topic in the *DMA Administration Guide*.

- Licenses for SQL Server and DMA.

For additional requirements, see the following Microsoft documentation:

SQL Server version	Microsoft documentation
2008	Hardware and Software Requirements for Installing SQL Server 2008
2008 R2	Hardware and Software Requirements for Installing SQL Server 2008 R2
2012	Hardware and Software Requirements for Installing SQL Server 2012

How this workflow works

This workflow creates a new database on the target instance.

Steps Executed

The MS SQL - Create Database workflow includes the following steps. Each step must complete successfully before the next step can start. If a step fails, the workflow reports a failure and all subsequent steps are skipped.

Steps used by MS SQL - Create Database

Workflow Step	Description
MS SQL Parameters Create Database v2	Gather and validate parameters for Create Database workflow.
MS SQL Advanced Parameters Create Database v2	Gather and validate optional parameters for Create Database workflow.
MS SQL Check Database Exists	Validates existence of database.
MS SQL Kill Processes	Kills all currently running user processes.
MS SQL Validate Directory Paths	Validates a comma-delimited string of directory paths.
MS SQL Drop Database	Drops target database. Ensure that there are no active connections prior to running this step by running the "MS SQL: Kill Processes" step.
MS SQL Validate Directory Paths	Validates a comma-delimited string of directory paths.
MS SQL Verify Server Login	Validates SQL server logins as well as Windows-authenticated server logins.
MS SQL Create Database	Creates a new database on the target Instance.
MS SQL Create Server Login	Validates a comma-delimited string of directory paths.
MS SQL Change Database Owner	Changes owner of target database to specified login.
MS SQL Change	Changes the recovery model of the target database.

Steps used by MS SQL - Create Database, continued

Workflow Step	Description
Recovery Model	
MS SQL Set Database Options	This step evaluates a comma-delimited list of option and value pairs, and sets the various database options.
Discover SQL Databases	Audits the server's physical environment looking for SQLServer instances and databases.

How to run this workflow

The following instructions show you how to customize and run the MS SQL - Create Database workflow in your environment.

The workflow provides default values for some parameters. These default values are usually sufficient for a "typical" installation. You can override the defaults by specifying parameter values in the deployment. You can also expose additional parameters in the workflow, if necessary, to accomplish more advanced scenarios. Any parameters not explicitly specified in the deployment will have the default values listed in ["Parameters for MS SQL - Create Database" on page 703](#).

Note: Before following this procedure, review the ["Prerequisites" on page 699](#), and ensure that all requirements are satisfied.

To use the MS SQL - Create Database workflow:

1. Create a deployable copy of the workflow (see "Create a Deployable Workflow" in *DMA Quick Start Tutorial*)
 - a. Determine the values that you will specify for the following parameters.

The following tables describe the required and optional input parameters for this workflow.

Step: MS SQL Parameters Create Database

Parameter	Description	Example Value
Database Name	Required: Name of the new database.	NewDatabase

Step: MS SQL Advanced Parameters Create Database

Parameter	Description	Example Value
Additional Database Options and Values		?

Step: MS SQL Advanced Parameters Create Database, continued

Parameter	Description	Example Value
Collation		?
Compatibility Level		?
Data File Paths		?
Data File Sizes, Growths, and Max Sizes	Comma-delimited list of sizing information for each data file. Optional, String. Blank values in list replaced with server defaults (3MB, 1MB, 0), depending on corresponding value. Values in list are initial size, growth increment, and max size, in that order. First 3 values in list apply to first data file, while next 3 apply to the next data file, and so on. Sizes expressed as [integer] [KB, MB, GB], growth rates expressed as [integer] [KB, MB, GB, %] or 0 (unlimited).	3MB, 1MB, 0
Data Filegroups	Comma-delimited list of filegroup (s) associated with data files. Optional, String. Blank values in list replaced with "PRIMARY".	PRIMARY
Database Owner Login Name	Login name of owner of the database. Optional, String. Windows authenticated login format: [domain]\[username]	?
Database Owner Login Password	The password of new owner of database. *Required (if new SQL login needed), String.	?
Database Recovery Model	Database recovery model. Optional, String. Acceptable values = [FULL (default), BULK_LOGGED, SIMPLE].	?
Default Database		?
Drop Database If Exists	Flag database as droppable if found. Optional, String. Acceptable inputs = YES, NO (default).	NO
Instance Account	Optional: The Windows account that will terminate the SQL Server processes.	
Instance Password	?	?
Log File Path	Directory path, file path, or	?

Step: MS SQL Advanced Parameters Create Database, continued

Parameter	Description	Example Value
	filename for log file. Optional, String. If blank, replaced with path [server default log directory]\[dbname]_log.mdf. Acceptable values = directory path (filename [DBname]_log.ldf used), file path, filename (default log directory used), or blank.	
Log File Size,Growth,and Max Size	Comma-delimited list of sizing information for log file. Optional, String. Blank items replaced with server defaults (3MB,1%,0), depending on corresponding value. The values in list are initial size, growth increment, and max size, in that order.	?

2. In the workflow editor, expose any additional parameters that you need. You will specify values for those parameters when you create the deployment or at runtime.
3. Save the changes to the workflow (click **Save** in the lower right corner).
4. Create a new deployment. See "Create a Deployment" in *DMA Quick Start Tutorial* for instructions.
5. On the Parameters tab, specify values (or set the type to Runtime Value) for the required parameters listed in step 2 and any additional parameters that you have exposed. You do not need to specify values for those parameters whose default values are appropriate for your environment.
6. On the Targets tab, specify one or more targets for this deployment.
7. Save the deployment (click **Save** in the lower right corner).
8. Run the workflow using this deployment, specifying any runtime parameters. See "Run Your Workflow" in (*DMA Quick Start Tutorial* for instructions.

To verify the results:

The workflow will complete and report SUCCESS on the Console if it has run successfully. If an error occurs during workflow execution, the error is logged, and the workflow terminates in the FAILURE state.

Parameters for MS SQL - Create Database

The following tables describe the required and optional input parameters for this workflow.

Step: MS SQL Parameters Create Database

Parameter	Required	Example Value	Description
Database Name	required	NewDatabase	Name of the new database.

Step: MS SQL Advanced Parameters Create Database

Parameter	Required	Example Value	Description
Additional Database Options and Values	NA	?	
Collation	NA	?	
Compatibility Level	NA	?	
Data File Paths	NA	?	
Data File Sizes, Growths, and Max Sizes		3MB,1MB,0	Comma-delimited list of sizing information for each data file. Optional, String. Blank values in list replaced with server defaults (3MB,1MB,0), depending on corresponding value. Values in list are initial size, growth increment, and max size, in that order. First 3 values in list apply to first data file, while next 3 apply to the next data file, and so on. Sizes expressed as [integer][KB,MB,GB], growth rates expressed as [integer][KB,MB,GB,%] or 0 (unlimited).
Data Filegroups		PRIMARY	Comma-delimited list of filegroup(s) associated with data files. Optional, String. Blank values in list replaced with "PRIMARY".
Database Owner Login Name		?	Login name of owner of the database. Optional, String. Windows authenticated login format: [domain]\[username]
Database Owner Login Password		?	The password of new owner of database. *Required (if new SQL login needed), String.
Database Recovery Model		?	Database recovery model. Optional, String. Acceptable values = [FULL (default),BULK_LOGGED,SIMPLE].
Default Database		?	
Drop Database If Exists		NO	Flag database as droppable if found. Optional, String. Acceptable inputs = YES, NO (default).
Instance Account			Optional: The Windows account that will terminate the SQL Server processes.

Step: MS SQL Advanced Parameters Create Database, continued

Parameter	Required	Example Value	Description
Instance Password		?	?
Log File Path		?	Directory path, file path, or filename for log file. Optional, String. If blank, replaced with path [server default log directory]\[dbname]_log.mdf. Acceptable values = directory path (filename [DBname]_log.ldf used), file path, filename (default log directory used), or blank.
Log File Size,Growth,and Max Size		?	Comma-delimited list of sizing information for log file. Optional, String. Blank items replaced with server defaults (3MB,1%,0), depending on corresponding value. The values in list are initial size, growth increment, and max size, in that order.

Sybase

This section includes the following topics:

Workflow type	Workflow name
Compliance	"Sybase - Compliance Audit v2" on the next page
Start or stop database	"Dump Sybase Database" on page 726
	"Load Sybase Database Dump" on page 740
	"Dump And Load Sybase Database" on page 754
	"Sybase - Start or Stop Instance" on page 772
Provisioning	"Provision Sybase ASE 15 Server" on page 836
	"Configure Sybase ASE 15 Server" on page 848
	"Create Sybase Database" on page 854
Release management	"Sybase Release Management" on page 778
Patching	"Sybase - Patch to Home and Instance" on page 798
	"Sybase - Rollback from Home and Instance" on page 822

Sybase - Compliance Audit v2

The "Sybase - Compliance Audit v2" workflow enables you to audit a Sybase Adaptive Server Enterprise instance for compliance with the following security benchmark requirements:

- Center for Internet Security (CIS) security configuration benchmarks
- Payment Card Industry (PCI) data security standard
- Sarbanes-Oxley (SOX) requirements

The workflow performs CIS Level 1 and Level 2 auditing for a Sybase ASE instance. The audit identifies up to 31 compliance related problems with a Sybase ASE instance.

The workflow performs the checks included in the CIS benchmark and then maps those CIS checks to the benchmark type that you specify in the Compliance Type parameter. The audit summary email will match the Compliance Type that you specify.

For links to the CIS, PCI, and SOX standards, see [Sybase Adaptive Server Enterprise \(ASE\) 15.0, version 1.1.0 \(December 2011\)](#).

To use this workflow in your environment, see the following information:

Topic	Information Included
"Prerequisites for this Workflow"	List of prerequisites that must be satisfied before you can run this workflow
"How this Workflow Works"	Information about what the workflow does, including validation checks performed, steps executed, and step descriptions
"How to Run this Workflow"	Instructions for running this workflow in your environment
"Sample Scenarios"	Examples of typical parameter values for this workflow
Parameters	List of input parameters for this workflow

Prerequisites for this Workflow

Be sure that the following prerequisites are satisfied before you run the ["Sybase - Compliance Audit v2"](#) workflow:

- The latest DMA solution packs require the latest DMA platform. To use the latest solution packs, update the DMA platform. DMA10.50.001.000 solution packs are supported on DMA10.50.001.000 (and later).
- You have installed the Database Compliance solution pack.

This workflow runs against a Sybase ASE instance by default. You can also run it at the Database level, however, by making a copy and modifying the `Target Level`.

This workflow requires unchallenged `sudo` access to a user (typically `root`) who can access all required files and directories.

`isql` must be installed and accessible via the user/password settings stored in metadata. You may find these setting in the Environment screen.

For more information about prerequisites for Sybase Adaptive Server Enterprise, refer to the [Sybase Adaptive Server Enterprise Documentation](#).

How this Workflow Works

This workflow performs the following actions:

- Prepares to run the workflow by gathering information about the target Sybase Adaptive Server Enterprise instance and validating parameter values.
- Audits the various configuration settings specified in the pertinent CIS, SOX, or PCI benchmark.
- Composes and sends an email containing the results of the audit.

Note: The emails are sent through the mail server configured on the DMA server. You can configure the mail server in the path below:

DMA setup > Configuration > Outgoing Mail > Server.

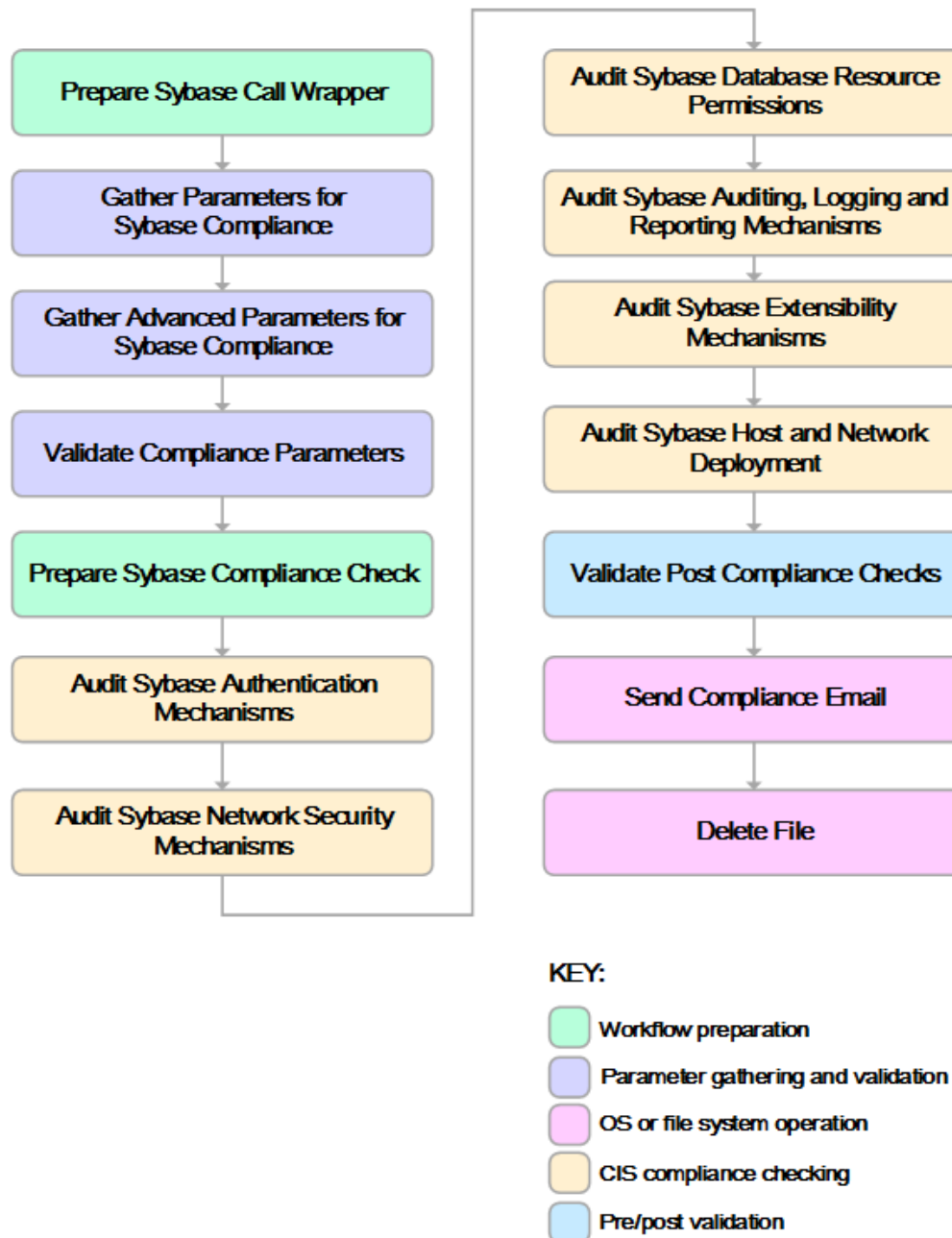
Validation Checks Performed

This workflow validates the following conditions:

1. Any Excluded Checks specified by the user refer to actual CIS, SOX, or PCI benchmark checks.
2. Any email addresses specified are valid addresses.
3. The workflow can create the temporary file that will store the compliance check results.

Steps Executed

The "Sybase - Compliance Audit v2" workflow includes the following steps. Each step must complete successfully before the next step can start. If a step fails, the workflow reports a failure and all subsequent steps are skipped.



Steps Used by Sybase Compliance Audit

Workflow Step	Description
Prepare Sybase Call Wrapper	This step constructs the commands that will be used to execute subsequent workflow steps as either the OS administrative user or the owner of the Sybase ASE installation.
Gather Parameters for Sybase Compliance	This step gathers two types of information: the list of compliance checks to exclude from the audit, and basic information about the Sybase ASE installation.
Gather Advanced Parameters for Sybase Compliance	This step gathers the information that the workflow needs to create and deliver the compliance audit report via email. It also enables you to specify the passwords for the various Sybase ASE user roles.
Validate Compliance Parameters	<p>This step validates the input parameters specified in the previous steps. It validates the list of excluded checks to ensure that all specified checks in the list correspond to actual Center for Internet Security (CIS) benchmark items. It also validates the email information to ensure that all specified email addresses are valid.</p> <p>The step then creates the path to the temporary file that will store the results of the current audit as the workflow is running. This file is deleted after the audit report is sent.</p>
Prepare Sybase Compliance Check	This step checks for database connectivity, verifies that the list of checks to be excluded from this compliance audit is properly formatted, and verifies that the email addresses specified are properly formatted.
Audit Sybase Authentication Mechanisms	<p>This step audits the scorable recommendations in Section 1, Authentication Mechanisms, of the Center for Internet Security (CIS) Security Configuration Benchmark for Sybase Adaptive Server Enterprise (ASE) 15.0, version 1.1.0 (December 2011).</p> <p>Checks not implemented: 1.5 - Remove unused accounts and change default passwords</p>
Audit Sybase Network Security Mechanisms	This step audits the scorable recommendations in Section 2, Network Security Mechanisms, of the Center for

Steps Used by Sybase Compliance Audit, continued

Workflow Step	Description
	Internet Security (CIS) Security Configuration Benchmark for Sybase Adaptive Server Enterprise (ASE) 15.0, version 1.1.0 (December 2011).
Audit Sybase Database Resource Permissions	This step audits the scorable recommendations in Section 3, Database Resource Permissions, of the Center for Internet Security (CIS) Security Configuration Benchmark for Sybase Adaptive Server Enterprise (ASE) 15.0, version 1.1.0 (December 2011).
Audit Sybase Auditing, Logging and Reporting Mechanisms	This step audits the scorable recommendations in Section 4, Auditing, Logging and Reporting Mechanisms, of the Center for Internet Security (CIS) Security Configuration Benchmark for Sybase Adaptive Server Enterprise (ASE) 15.0, version 1.1.0 (December 2011).
Audit Sybase Extensibility Mechanisms	This step audits the scorable recommendations in Section 5, Extensibility Mechanisms, of the Center for Internet Security (CIS) Security Configuration Benchmark for Sybase Adaptive Server Enterprise (ASE) 15.0, version 1.1.0 (December 2011)
Audit Sybase Host and Network Deployment	This step audits the scorable recommendations in Section 6, Host and Network Deployment, of the Center for Internet Security (CIS) Security Configuration Benchmark for Sybase Adaptive Server Enterprise (ASE) 15.0, version 1.1.0 (December 2011)
Validate Post Sybase Compliance Checks	This step reads the temporary file that contains the results of the compliance audit and prints the audit results to the DMA Console. It also creates (or updates) the compliance metadata fields for the target. If email addresses were specified, it also creates a report in HTML format that will be emailed to those addresses by a later step in the workflow.
Send Compliance Email	If email addresses are provided, this step sends the previously generated compliance audit report to the specified email addresses.
Delete File	This step deletes the specified file on the target server.

Note: For input parameter descriptions and defaults, see "[Parameters for Sybase - Compliance Audit](#)" on page 723.

How to Run this Workflow

The following instructions show you how to customize and run the ["Sybase - Compliance Audit v2"](#) workflow in your environment.

The workflow provides default values for some parameters. These default values are usually sufficient for a "typical" installation. You can override the defaults by specifying parameter values in the deployment. You can also expose additional parameters in the workflow, if necessary, to accomplish more advanced scenarios. Any parameters not explicitly specified in the deployment will have the default values listed in ["Parameters for Sybase - Compliance Audit" on page 723](#).

Note: Before following this procedure, review the ["Prerequisites for this Workflow" on page 708](#), and ensure that all requirements are satisfied.

To use the Run Sybase Compliance Audit workflow:

1. Create a deployable copy of the workflow.
2. Determine the values that you will specify for the following parameters:

Parameters Defined in this Step: Prepare Sybase Call Wrapper

Parameter Name	Default Value	Required	Description
Call Wrapper	see description	optional	Command that will execute this step (or subsequent steps) as a specific user. For UNIX targets, the default is: <code>/opt/hp/dma/client/jython.sh</code> running as root For Windows targets, the default is: <code>jython</code> running as Administrator
Sybase OS User Name	sybase	required	OS user who owns the Sybase ASE installation directory.

Parameters Defined in this Step: Gather Parameters for Sybase Compliance

Parameter Name	Default Value	Required	Description
Excluded Compliance Checks	no default	optional	Comma-separated list of compliance checks to exclude from the audit. For example: <code>1.2, 2, 3.*, 5*, 6.1.2</code> Note: Make sure that the checks specified here correspond with the compliance audit type (CIS, PCI, or SOX) that you are running.

Parameters Defined in this Step: Gather Advanced Parameters for Sybase Compliance

Parameter Name	Default Value	Required	Description
Compliance Type	CIS	optional	Type of compliance report that will be generated by the workflow. Supported types are: CIS = Center for Internet Security (CIS) Security Configuration Benchmark PCI = Payment Card Industry (PCI) Data Security Standard SOX = Sarbanes-Oxley (SOX) sections 302.2, 302.4b, 302.4c, and 302.5 requirements
Email Addresses to Receive Report	no default	optional	Comma-separated list of email addresses for those individuals or groups who will receive a copy of the compliance audit report.

Parameters Defined in this Step: Audit Sybase Host and Network Deployment

Parameter Name	Default Value	Required	Description
EBF Patch Level	no default	optional	Latest Express Bug Fix (EBF) patch level available from Sybase.
ESD Patch Level	no default	optional	Latest Electronic Software Distribution (ESD) patch level available from Sybase.

Note: This is the minimum set of parameters required to run this workflow. You may need to expose additional parameters depending on your objectives.

See ["Parameters for Sybase - Compliance Audit" on page 723](#) for detailed descriptions of all input parameters for this workflow, including default values.

3. In the workflow editor, expose any additional parameters that you need. You will specify values for those parameters when you create the deployment.
4. Save the changes to the workflow (click **Save** in the lower right corner).
5. Create a new deployment.
6. On the Parameters tab, specify values for the required parameters listed in step 2 and any additional parameters that you have exposed. You do not need to specify values for those parameters whose default values are appropriate for your environment.
7. On the Targets tab, specify one or more targets for this deployment.
8. Save the deployment (click **Save** in the lower right corner).
9. Run the workflow using this deployment.

To verify the results:

Information about each compliance check is displayed in the step output on the Console (and the History page) for each of the audit steps.

A summary of the compliance audit is also displayed in the step output for the Validate Post Sybase Compliance Checks step.

To view the reports:

A compliance audit summary in HTML format is emailed to all parties on the Email Addresses to Receive Report list.

After you run this workflow, you can generate two types of compliance reports on the Reports page:

- Database Compliance Report
- Database Compliance Detail Report

To access the Database Compliance reports:

1. Go to the Reports page.
2. At the bottom of the page, specify the following settings:

For the Database Compliance Report:

- a. Select the Database Compliance report.
- b. Select the organization where your target resides.
- c. Because this report lists the latest compliance audit reports for all targets in the specified organization, you do not specify a Server, Database, or Time span.

For the Database Compliance Detail Report:

- a. Select the Database Compliance Details report.
- b. Select the organization where your target resides.
- c. Specify the Server and Instance that you selected when you created your deployment.

3. Click **Run report**.

Sample Scenarios

This topic shows you how to use various parameters to achieve the following compliance audit scenarios in your environment using the "Sybase - Compliance Audit v2" workflow.

Scenario 1: Perform a Partial CIS Compliance Audit and Email the Results

In the scenario, the following checks are excluded from the audit:

- Section 5: Extensibility Mechanisms
- Section 6: Host and Network Deployment

A summary report is sent to the three parties listed in the Email Addresses to Receive Report parameter.

Parameter Name	Example Value	Description
Excluded Compliance Checks	5.*,6.*	<p>Comma-separated list of compliance checks to exclude from the audit. For example:</p> <p>1.2, 2, 3.*, 5*, 6.1.2</p> <p>Note: Make sure that the checks specified here correspond with the compliance audit type (CIS, PCI, or SOX) that you are running.</p>
Compliance Type	CIS	<p>Type of compliance report that will be generated by the workflow. Supported types are:</p> <p>CIS = Center for Internet Security (CIS) Security Configuration Benchmark</p> <p>PCI = Payment Card Industry (PCI) Data Security Standard</p> <p>SOX = Sarbanes-Oxley (SOX) sections 302.2, 302.4b, 302.4c, and 302.5 requirements</p>
Email Addresses to Receive Report	SybaseDBAdminTeam@mycompany.com, SybaseDBAdminMgr@mycompany.com, CustomerSupportTeam@mycompany.com	Comma-separated list of email addresses for those individuals or groups who will receive a copy of the compliance audit report.

Be sure that the default values for all remaining input parameters are appropriate for your environment (see ["Parameters for Sybase - Compliance Audit" on page 723](#)).

Scenario 2: Perform a Full PCI Compliance Audit and Email the Results

A summary report is sent to the three parties listed in the Email Addresses to Receive Report parameter.

Parameter Name	Example Value	Description
Compliance Type	PCI	<p>Type of compliance report that will be generated by the workflow. Supported types are:</p> <p>CIS = Center for Internet Security (CIS) Security Configuration Benchmark</p> <p>PCI = Payment Card Industry (PCI) Data Security Standard</p> <p>SOX = Sarbanes-Oxley (SOX) sections 302.2, 302.4b, 302.4c, and 302.5 requirements</p>
Email Addresses to Receive Report	SybaseDBAdminTeam@mycompany.com, SybaseDBAdminMgr@mycompany.com, CustomerSupportTeam@mycompany.com	Comma-separated list of email addresses for those individuals or groups who will receive a copy of the compliance audit report.

Note: Some of these parameters are not exposed by default in the deployment.

Be sure that the default values for all remaining input parameters are appropriate for your environment (see "[Parameters for Sybase - Compliance Audit](#)" on page 723).

Scenario 3: Perform a Full SOX Compliance Audit and Email the Results

A summary report is sent to the three parties listed in the Email Addresses to Receive Report parameter.

Parameter Name	Example Value	Description
Compliance Type	SOX	Type of compliance report that will be generated by the workflow. Supported types are: CIS = Center for Internet Security (CIS) Security Configuration Benchmark PCI = Payment Card Industry (PCI) Data Security Standard SOX = Sarbanes-Oxley (SOX) sections 302.2, 302.4b, 302.4c, and 302.5 requirements
Email Addresses to Receive Report	SybaseDBAdminTeam@mycompany.com, SybaseDBAdminMgr@mycompany.com, CustomerSupportTeam@mycompany.com	Comma-separated list of email addresses for those individuals or groups who will receive a copy of the compliance audit report.

Note: Some of these parameters are not exposed by default in the deployment.

Be sure that the default values for all remaining input parameters are appropriate for your environment.

Scenario 4: Perform a Full CIS Compliance Audit and Display the Results on the DMA Console

In the scenario, all scorable checks are performed, and the compliance audit report is displayed only on the DMA Console. In this case, a summary report is not emailed. This scenario would be appropriate for initial testing.

It is not necessary to specify any input parameters in this scenario unless the Sybase ASE inventory file is located in a non-standard directory.

Parameter Name	Example Value	Description
Compliance Type	CIS	Type of compliance report that will be generated by the workflow. Supported types are: CIS = Center for Internet Security (CIS) Security Configuration Benchmark PCI = Payment Card Industry (PCI) Data Security Standard SOX = Sarbanes-Oxley (SOX) sections 302.2, 302.4b, 302.4c, and 302.5 requirements

Be sure that the default values for all remaining input parameters are appropriate for your environment (see ["Parameters for Sybase - Compliance Audit" on the next page](#)).

Parameters for Sybase - Compliance Audit

The following tables describe the required and optional input parameters for this workflow. Some of these parameters are not initially visible in a deployment. For most parameters, if you do not specify a value for a parameter, a default value is assigned.

Parameters Defined in this Step: Prepare Sybase Call Wrapper

Parameter Name	Default Value	Required	Description
Call Wrapper	see description	optional	Command that will execute this step (or subsequent steps) as a specific user. For UNIX targets, the default is: /opt/hp/dma/client/jython.sh running as root For Windows targets, the default is: jython running as Administrator
Sybase OS User Name	sybase	required	OS user who owns the Sybase ASE installation directory.

Additional Parameters Defined in this Step: Gather Parameters for Sybase Compliance

Parameter Name	Default Value	Required	Description
Excluded Compliance Checks	no default	optional	Comma-separated list of compliance checks to exclude from the audit. For example: 1.2, 2, 3.*, 5*, 6.1.2 Note: Make sure that the checks specified here correspond with the compliance audit type (CIS, PCI, or SOX) that you are running.

Additional Parameters Defined in this Step: Gather Advanced Parameters for Sybase Compliance

Parameter Name	Default Value	Required	Description
Compliance Type	CIS	optional	Type of compliance report that will be generated by the workflow. Supported types are: CIS = Center for Internet Security (CIS) Security Configuration Benchmark PCI = Payment Card Industry (PCI) Data Security Standard SOX = Sarbanes-Oxley (SOX) sections 302.2, 302.4b, 302.4c, and 302.5 requirements

Additional Parameters Defined in this Step: Gather Advanced Parameters for Sybase Compliance, continued

Parameter Name	Default Value	Required	Description
Email Addresses to Receive Report	no default	optional	Comma-separated list of email addresses for those individuals or groups who will receive a copy of the compliance audit report.
OPER Role Password	no default	optional	Password for the Sybase ASE oper_role (operator) role.
SA Role Password	no default	optional	Password for the Sybase ASE sa_role (system administrator) role.
SSO Role Password	no default	optional	Password for the Sybase ASE sso_role (system security officer) role.
Sybase Role Password	no default	optional	Password for the sybase_ts_role (Sybase technical support) role.
List Of Used Accounts	no default	optional	Comma separated list of user accounts that need to be retained and are in use. For example: probe,sybmail,jstask,mon_user.
Sybase Dump File List	no default	optional	List of dump files to be checked for password-protection. For example: /opt/app/sybase/data/somedump1.dmp, /opt/app/sybase/data/somedump2.dmp, /opt/app/sybase/data/somedump3.dmp.

Additional Parameters Defined in this Step: Audit Sybase Host and Network Deployment

Parameter Name	Default Value	Required	Description
EBF Patch Level	no default	optional	Latest Express Bug Fix (EBF) patch level available from Sybase.
ESD Patch Level	no default	optional	Latest Electronic Software Distribution (ESD) patch

Additional Parameters Defined in this Step: Audit Sybase Host and Network Deployment, continued

Parameter Name	Default Value	Required	Description
			level available from Sybase.

Dump Sybase Database

This workflow enables you to dump the contents of a Sybase Adaptive Server Enterprise (ASE) database (the source database) into a file (the database dump file).

The workflow performs extensive validation checks prior to and immediately after the dump operation to ensure that the dump file is valid.

This workflow can create and load database dump files that are striped, compressed (at any level 1-9), encrypted, or any combination thereof.

If any source database objects are bound to a specific (non-default) cache, the workflow will create a cache dump file—provided that you specify a valid value for the Cache Dump File parameter. The cache dump file contains details about the specific caches used by the source database and any objects that are bound to each cache. This file is in data-readable format.

To use this workflow in your environment, see the following information:

Topic	Information Included
"Prerequisites for this Workflow"	List of prerequisites that must be satisfied before you can run this workflow
"How this Workflow Works"	Information about what the workflow does, including validation checks performed, steps executed, and a high-level process flow
"How to Run this Workflow"	Instructions for running this workflow in your environment
"Sample Scenarios"	Examples of typical parameter values for this workflow
"Parameters for Dump Sybase Database"	List of input parameters for this workflow

The process of deploying and running this workflow is the same for all scenarios, but the parameters required will differ depending on the specific scenario that you are implementing.

The workflow provides default values for most parameters. These default values are usually sufficient for a "typical" database refresh. You can override the defaults by specifying parameter values in the deployment. You can also expose additional parameters in the workflow, if necessary, to accomplish more advanced scenarios.

Any parameters not explicitly specified in the deployment will have the default values listed in ["Parameters for Dump Sybase Database" on page 737](#).

Note: To view detailed information about the steps included in this workflow, see the [Steps in this Workflow](#).

Prerequisites for this Workflow

Caution: You cannot perform a database dump if there are dependencies between the source database and another database in the same or a different Sybase ASE instance. You must remove or disable object referencing (for example: triggers, views, stored procedures, etc.) before you run this workflow.

The following prerequisites must be satisfied before you can run the Dump Sybase Database workflow:

1. The **source** database must exist before the workflow runs.
2. The source database must NOT be mounted on the master device.
3. Both the Adaptive Server instance that executes the dump command and the local Backup Server instance must be running, and they must be able to communicate with each other.
4. The master database system table (sys.servers) must contain an entry that assigns the local Backup Server instance to SYB_BACKUP.
5. By default, the workflow will create the database dump file with the following format:

`dump_file_path/<databaseName>_<dateTime>.dmp`

For example: `/var/tmp/mytestdb_2012111283762.dmp`

If you specify a non-default file name (or names) in the Dump File List parameter, the path to each specified file must exist.

6. Adequate disk space must be available to store the database dump file, whether it is stored locally or in a shared NFS location.
7. On Linux and Solaris platforms, the `sudo` package must be installed on the server that hosts the source database.
8. The Dump File Password parameter is required if a password was used to encrypt the **source** database dump file.
9. The workflow assumes the following:
 - The Adaptive Server component is installed in the `/home/Sybase/ASE_15` directory.
 - The Adaptive Server instance name is `NY_DS`.
 - The database name is `mytestdb`.
 - The database dump file is stored in the `/var/tmp` directory.
 - `/var/tmp` is an NFS mount point.
 - The Sybase ASE user specified in the ASE SysAdmin Username parameter is permitted to

access the `/var/tmp` directory.

- The user specified in the Sybase OS User Name parameter (sybase by default) must own the installation directory and be a member of the “sybase” group.

Note: The workflow currently does not support reading the database dump file from tape devices.

Note: This workflow does not support dump file password encryption for **cross-platform** database refresh (for example: the database dump file was created on a Linux server, and you are loading it onto a Solaris server).

Additional Considerations

It is good practice to run basic database consistency checks (DBCCs) on the source database before running this workflow. You can do this by creating a simple workflow that includes the Run Sybase DBCC Checks step included in this solution pack.

If database transactions occur on the source database after the dump file is created, you should apply the latest transaction log dump to the destination database after you run the ["Load Sybase Database Dump"](#) workflow. Otherwise, these transactions will be missing from the destination database.

For information about prerequisites for Sybase ASE, refer to the [Sybase ASE Product Documentation](#).

How this Workflow Works

This topic contains information about the "Dump Sybase Database" workflow:

Validation Checks Performed

The workflow checks the following things prior to dumping the database. If any of these checks fails, the workflow fails.

1. All required parameters have values. If any required parameter does not have a value—either a value that you specify or a default value—the workflow fails in the Sybase - Validate Database Dump Settings step.
2. The Sybase ASE software is installed.
3. The source database exists in the specified Sybase ASE instance.
4. The source Adaptive Server and Backup Server components are running and able to communicate with each other so that they can perform the database dump.
5. The **source** database is online.
6. Adequate disk space is available to store the database dump file.

Steps Executed

The "Dump Sybase Database" workflow includes the following steps. Each step must complete successfully before the next step can start. If a step fails, the workflow reports a failure, and all subsequent steps are skipped.

Process Flow

This workflow performs the following tasks:

1. Creates the Instance Wrapper and Server Wrapper.
2. Verifies that the DMAserver is able to communicate with the server where the workflow is running.
3. Performs the preliminary **validation checks** described above.
4. Generates the cache descriptor file for the source database. This is used to replicate the cache objects on the destination server.
5. Performs the database dump operation to create the database dump file.
6. Performs post-dump validation checks to ensure that all required parameters had valid values.

Tips and Best Practices

It is good practice to run basic database consistency checks (DBCCs) on the source database before running this workflow to ensure that there are no internal errors in the database. You can do this by creating a simple workflow that includes the Run Sybase DBCC Checks step included in this solution pack.

If you find errors in the source database, be sure to fix them before running this workflow. The workflow does not have the ability to diagnose or remediate problems in the database prior to performing the database dump.

How to Run this Workflow

This topic explains how to customize and run the "Dump Sybase Database" workflow in your environment.

Note: Prior to running this workflow, review the "Prerequisites for this Workflow", and ensure that all requirements are satisfied.

To customize and run the Dump Sybase Database workflow:

1. Create a deployable copy of the workflow.
2. Determine the values that you will specify for the following parameters. This is the minimum set of parameters required to run this workflow.

Parameter Name	Default Value	Description
Call Wrapper	jython	Command that will be used to construct the call wrapper. The workflow uses the call wrapper to execute subsequent steps as either the OS administrative user (for example: <code>sudo su - root /opt/hp/dma/client/bin/jython.sh</code>) or the owner of the Sybase ASE installation (for example: <code>sudo su - sybase /opt/hp/dma/client/bin/jython.sh</code>).
Sybase OS User Name	sybase	OS user (typically, sybase) who owns the Sybase ASE installation directory.
Cache File	no default	Database cache file associated with this database dump. This is a single filename (with absolute path—path must exist). The file contains detailed information about any specific (non-default) data caches used by the source database and any database objects bound to those caches.
Dump File Compression Level	7	Compression level (1-9) to apply to the dump file (or files) that will be created.
Dump File Password	no default	Password required to decrypt a password-protected encrypted database dump file (required if the dump file is encrypted). Note: You cannot use an encrypted dump file to perform a

Parameter Name	Default Value	Description
		cross-platform refresh when an architectural endian difference exists (for example: create dump on Linux, load dump on Solaris).

Note: This is the minimum set of parameters required to run this workflow. You may need to expose additional parameters depending on your objectives.

See ["Parameters for Dump Sybase Database" on page 737](#) for detailed descriptions of all input parameters for this workflow, including default values.

To avoid having to re-enter passwords whenever they change, you can create a policy to provide them to the workflow.

3. In the workflow editor, expose any additional parameters that you need (see [How to Expose Additional Workflow Parameters on page 70](#)). You will specify values for those parameters when you create the deployment.
4. Save the changes to the workflow (click **Save** in the lower right corner).
5. Create a new deployment.
6. On the **Parameters** tab, specify values for the required parameters listed in step 2 and any additional parameters that you have exposed. You do not need to specify values for those parameters whose default values are appropriate for your environment.
7. On the **Targets** tab, specify one or more targets for this deployment.
8. Save the deployment (click **Save** in the lower right corner).
9. Run the workflow using this deployment.

The workflow will complete and report "Success" on the Console if it has run successfully. If an invalid parameter value is specified, an error is logged, and the workflow terminates in the "Failure" state.

Sample Scenarios

This topic shows you how to use various parameters to achieve the following database refresh scenarios in your environment using the "Dump Sybase Database" workflow:

Scenario 1: Perform a Database Refresh Using a Database Dump File that is Not Encrypted or Striped

This is the simplest Sybase ASE database dump scenario.

Parameter Name	Example Value	Description
Call Wrapper	jython	Command that will be used to construct the call wrapper. The workflow uses the call wrapper to execute subsequent steps as either the OS administrative user (for example: <code>sudo su - root /opt/hp/dma/client/bin/jython.sh</code>) or the owner of the Sybase ASE installation (for example: <code>sudo su - sybase /opt/hp/dma/client/bin/jython.sh</code>).
Sybase OS User Name	sybase	OS user (typically, sybase) who owns the Sybase ASE installation directory.

Be sure that the default values for all remaining parameters are appropriate for your environment (see Parameters for Dump Sybase Database).

Scenario 2: Perform a Database Refresh Using a Database Dump File that is Encrypted and Compressed

This scenario requires you to specify the encryption password and compression level for the database dump file.

Parameter Name	Example Value	
Call Wrapper	jython	Command that will be used to construct the call wrapper. The workflow uses the call wrapper to execute subsequent steps as either the OS administrative user (for example: <code>sudo su - root /opt/hp/dma/client/bin/jython.sh</code>) or the owner of the Sybase ASE installation (for example: <code>sudo su - sybase /opt/hp/dma/client/bin/jython.sh</code>).
Sybase OS User Name	sybase	OS user (typically, sybase) who owns the Sybase ASE installation directory.
Dump File Compression Level	8	Compression level (1-9) to apply to the dump file (or files) that will be created.
Dump File Password	MyPassword1@#	<p>Password that will be used to encrypt the database dump file.</p> <p>Note: You cannot use an encrypted dump file to perform a cross-platform refresh when an architectural endian difference exists (for example: create dump on Linux, load dump on Solaris).</p>

Be sure that the default values for all remaining parameters are appropriate for your environment (see ["Parameters for Dump Sybase Database" on page 737](#)).

Scenario 3: Perform a Database Refresh Using a Database Dump File that is Striped and Encrypted

In this scenario, the database dump file will be striped across multiple files. You must specify all the individual stripe files in the Dump File List parameter (separate them with commas).

If you want the stripe files to be encrypted, you must also specify the Dump File Password parameter.

Parameter Name	Example Value	Description
Call Wrapper	jython	Command that will be used to construct the call wrapper. The workflow uses the call wrapper to execute subsequent steps as either the OS administrative user (for example: <code>sudo su - root</code> <code>/opt/hp/dma/client/bin/jython.sh</code>) or the owner of the Sybase ASE installation (for example: <code>sudo su - sybase</code> <code>/opt/hp/dma/client/bin/jython.sh</code>).
Sybase OS User Name	sybase	OS user (typically, sybase) who owns the Sybase ASE installation directory.
Dump File List	<code>/var/tmp/mytestdb1.dmp,</code> <code>/var/tmp/mytestdb2.dmp,</code> <code>/var/tmp/mytestdb3.dmp</code>	Comma-separated list of database dump files (with absolute paths—all specified paths must exist). For a single dump file, no comma is necessary.
Dump File Password	MyPassword1@#	Password that will be used to encrypt the database dump file. Note: You cannot use an encrypted dump file to perform a cross-platform refresh when an architectural endian difference exists (for example: create dump on Linux, load dump on Solaris).

Be sure that the default values for all remaining parameters are appropriate for your environment (see ["Parameters for Dump Sybase Database" on page 737](#)).

Scenario 4: Perform a Database Refresh Using a Cache Dump File

In this scenario, the database dump file has an associated cache dump file. You must specify the name of the cache dump file by using the Cache File parameter. The workflow will use the cache dump file to rebuild and bind the cache after the database dump file is loaded into the destination database.

Parameter Name	Example Value	
Call Wrapper	jython	Command that will be used to construct the call wrapper. The workflow uses the call wrapper to execute subsequent steps as either the OS administrative user (for example: <code>sudo su - root /opt/hp/dma/client/bin/jython.sh</code>) or the owner of the Sybase ASE installation (for example: <code>sudo su - sybase /opt/hp/dma/client/bin/jython.sh</code>).
Sybase OS User Name	sybase	OS user (typically, sybase) who owns the Sybase ASE installation directory.
Dump File List	<code>/var/tmp/mytestdb1.dmp, /var/tmp/mytestdb2.dmp, /var/tmp/mytestdb3.dmp</code>	Comma-separated list of database dump files (with absolute paths—all specified paths must exist). For a single dump file, no comma is necessary.
Cache File	<code>/var/tmp/runcache_ mytestdb.txt</code>	File where the Sybase ASE database cache configuration data for the source database will be written. This is a single filename (with absolute path—path must exist).

Be sure that the default values for all remaining parameters are appropriate for your environment (see Parameters for Dump Sybase Database).

Parameters for Dump Sybase Database

The following tables describe the required and optional input parameters for this workflow. Most of these parameters are not initially visible in a deployment. For most parameters, if you do not specify a value for a parameter, a default value is assigned in the following steps:

- Gather Parameters for Sybase Dump or Load
- Gather Advanced Parameters for Sybase Database Dump

Input Parameters for the Dump Sybase Database Workflow

Parameter Name	Default Value	Required	Description
ASE SysAdmin Password	password	required	Password for the Sybase ASE user specified in the ASE SysAdmin Username parameter.
ASE SysAdmin Username	sa	required	The Sybase ASE user who can perform all administrative operations (typically sa). This user will perform the database load operation.
Cache File	no default	optional	Database cache file associated with this database dump. This is a single filename (with absolute path—the path and file must exist). The file contains detailed information about any specific (non-default) data caches used by the source database and any database objects bound to those caches.
Call Wrapper	jython	required	Command that will be used to construct the call wrapper. The workflow uses the call wrapper to execute subsequent steps as either the OS administrative user (for example: <code>sudo su - root /opt/hp/dma/client/bin/jython.sh</code>) or the owner of the Sybase ASE installation (for example: <code>sudo su - sybase /opt/hp/dma/client/bin/jython.sh</code>).
Dump Device Name	n/a	n/a	Not used in this release.
Dump File Compression Level	7	optional	Compression level (1-9) to apply to the dump file (or files) that will be created.
Dump File List	<code>/var/tmp/< databasename>_<datetime>.dmp</code> For example: <code>/var/tmp/mytestdb_2012111283762.dmp</code>	required	Comma-separated list of database dump files (with absolute paths—all specified paths must exist). For a single dump file, no comma is necessary.

Input Parameters for the Dump Sybase Database Workflow, continued

Parameter Name	Default Value	Required	Description
	If you specify a non-default file name (or names) in the Dump File List parameter, the path to each specified file must exist.		
Dump File Password	no default	optional	Password required to decrypt a password-protected encrypted database dump file (required if the dump file is encrypted). Note: You cannot use an encrypted dump file to perform a cross-platform refresh when an architectural endian difference exists (for example: create dump on Linux, load dump on Solaris).
Dump File Path	n/a	n/a	Not used in this release.
Local Backup Instance Name	n/a	n/a	Not used in this release.
Local Backup Instance Port	n/a	n/a	Not used in this release.
Remote Backup Instance Name	n/a	n/a	Not used in this release.
Remote Backup Instance Port	n/a	n/a	Not used in this release.
Role Password SQL Statement	no default	required	Not used in this release.
Source Database Instance Name	NY_DS	required	Name of the Adaptive Server instance where the dump file (or files) will be created. You specify the value of this parameter in the deployment.
Source Database Name	mytestdb	required	Name of database from which the dump file (or files) will be created.
Sybase ASE Home Directory	/home/sybase/ASE_15	required	Sybase ASE installation home directory, where the source database resides. Sybase will examine the interface file that exists in this

Input Parameters for the Dump Sybase Database Workflow, continued

Parameter Name	Default Value	Required	Description
			directory to determine how to create the specified database dump file (or files).
Sybase OS User Name	sybase	required	OS user (typically, sybase) who owns the Sybase ASE installation directory.

Load Sybase Database Dump

This workflow enables you to load the contents of a previously created Sybase ASE database dump file (the source data) into an existing Sybase ASE database (the destination database).

The workflow performs extensive validation checks prior to and immediately after loading the source data into the destination database to ensure that the schema and data have been loaded successfully. The workflow restores any existing database users after the source data is loaded into the destination database.

This workflow can perform a cross-platform database refresh (load) if necessary. After it performs a cross-platform load operation, the workflow rebuilds the indexes (clustered or non-clustered indexes on APL/DOL tables) to avoid any page linkage or index corruption issues.

The source database dump file (or files) can be striped, compressed (at any level 1-9), encrypted, or any combination thereof.

To use this workflow in your environment, see the following information:

Topic	Information Included
"Prerequisites for this Workflow"	List of prerequisites that must be satisfied before you can run this workflow
"How this Workflow Works"	Information about what the workflow does, including validation checks performed, steps executed, and a high-level process flow
"How to Run this Workflow"	Instructions for running this workflow in your environment
"Sample Scenarios"	Examples of typical parameter values for this workflow
"Parameters for Load Sybase Database Dump"	List of input parameters for this workflow

The process of deploying and running this workflow is the same for all scenarios, but the parameters required will differ depending on the specific scenario that you are implementing.

The workflow provides default values for most parameters. These default values are usually sufficient for a "typical" database refresh. You can override the defaults by specifying parameter values in the deployment. You can also expose additional parameters in the workflow, if necessary, to accomplish more advanced scenarios.

Any parameters not explicitly specified in the deployment will have the default values listed in ["Parameters for Load Sybase Database Dump" on page 751](#).

Note: To view detailed information about the steps included in this workflow, see [Steps in this Workflow](#).

Prerequisites for this Workflow

The following prerequisites must be satisfied before you can run the Load Sybase Database Dump workflow:

1. The **destination** database must exist before the workflow runs.
2. The destination database must NOT be mounted on the master device.
3. The **source** and destination database servers must use the same page size.
4. No database users may be logged in to the destination database server when this workflow runs.
5. Both the Adaptive Server instance that executes the `load` command and the local Backup Server instance must be running, and they must be able to communicate with each other.
6. The master database system table (sys.servers) must contain an entry that assigns the local Backup Server instance to SYB_BACKUP.
7. On Linux and Solaris platforms, the `sudo` package must be installed on the server that hosts the destination database.
8. You must specify an operating system file in the Dump File List parameter (for example: `/var/tmp/mydbdump.dmp`). You cannot specify a dump device.

The database dump file must be accessible from the server where the workflow is executed. The file must be available on the local machine or via a Network File System (NFS) mount.

The workflows currently do not support writing or reading the database dump file from tape devices.

9. The file (or files) specified in the Dump File List parameter must exist in the specified location.
10. The Dump File Password parameter is required if a password was used to encrypt the source database dump file.
11. The workflow assumes the following:
 - The Adaptive Server component is installed in the `/home/sybase/ASE_15` directory.
 - The Adaptive Server instance name is NY_DS.
 - The database name is mytestdb.
 - The database dump file is stored in the `/var/tmp` directory.
 - `/var/tmp` is an NFS mount point.
 - The Sybase ASE user specified in the ASE SysAdmin Username parameter is permitted to access the `/var/tmp` directory.

- The user specified in the Sybase OS User Name parameter (sybase by default) must own the installation directory and be a member of the "sybase" group.

Note: The workflow currently does not support reading the database dump file from tape devices.

Note: This workflow does not support dump file password encryption for **cross-platform** database refresh (for example: the database dump file was created on a Linux server, and you are loading it onto a Solaris server).

Additional Considerations

It is good practice to run basic database consistency checks (DBCCs) on the source database before running this workflow. You can do this by creating a simple workflow that includes the Run Sybase DBCC Checks step included in this solution pack.

If database transactions occur on the source database after the dump file is created, you should apply the latest transaction log dump to the destination database after you run the ["Load Sybase Database Dump"](#) workflow. Otherwise, these transactions will be missing from the destination database.

For information about prerequisites for Sybase ASE, refer to the [Sybase ASE Product Documentation](#).

How this Workflow Works

This topic contains information about the ["Load Sybase Database Dump"](#) workflow:

Caution: You cannot refresh the target database (load the database dump) if there are dependencies between the target database and another database in the same or a different Sybase ASE instance. You must remove or disable object referencing (for example: triggers, views, stored procedures, etc.) before you run this workflow.

Validation Checks Performed

The workflow checks the following things prior to refreshing the database. If any of these checks fails, the workflow fails.

1. All required parameters have values. If any required parameter does not have a value—either a value that you specify or a default value—the workflow fails in the Sybase - Validate Database Refresh Settings step.
2. The Sybase ASE software is installed.
3. The target database and the Backup Server are running and able to communicate with each other.
4. The dump file server page size matches the target database server page size.
5. The Sybase ASE version in the database dump file header is compatible with the target Sybase ASE instance version. The following versions are compatible:

Dump File Version	Target Instance Version
Sybase ASE 15.0.3 or 15.5	Sybase ASE 15.0.3 or 15.5
Sybase ASE 12.5.4	Sybase ASE 15.0.3

6. The target database exists.
7. The size of the target database is sufficient to load the database dump file.

The workflow then determines whether the target database server is currently in use by Sybase ASE users. If the database is in use, the workflow creates a backup of the target database users and groups in tempdb before it refreshes the database. It restores the users after the database is refreshed.

Steps Executed

The ["Load Sybase Database Dump"](#) workflow includes the following steps. Each step must complete successfully before the next step can start. If a step fails, the workflow reports a failure, and all subsequent steps are skipped.

Process Flow

This workflow performs the following tasks:

1. Creates the Instance Wrapper and Server Wrapper.
2. Verifies that the DMAserver is able to communicate with the server where the workflow is running.
3. Performs the pre-refresh [validation checks](#) described above.
4. Reads the header of the database dump file, and validates that the source Sybase ASE page size matches the target Sybase ASE page size. The workflow fails if the page sizes do not match.
5. Backs up any existing database users and groups.
6. Determines whether the source (the database dump file) and target servers have different byte architectures (big-endian versus little-endian).
7. Enables the database level “`dbo use only`” option to ensure that no users except the database owner are accessing the destination database.
8. Loads the database dump file on the target database server, and refreshes the destination database.
9. Brings the destination database online and performs the post-refresh checks.
10. Rebuild the indexes using the Sybase ASE recommended `sp_post_xpload` system stored procedure.
11. Runs the specified database consistency checker (DBCC) checks to ensure that no database tables or objects have become corrupted. The output of these checks is printed in the step log and stored in files under the specified directory.
12. Builds the specified cache (if specified), and binds the database object to either the default data cache or the specified cache.

Tips and Best Practices

It is good practice to run basic database consistency checks (DBCCs) on the source database before you create the dump file (or files) to ensure that there are no internal errors in the database. You can do this by creating a simple workflow that includes the Run Sybase DBCC Checks step included in this solution pack.

If you find errors in the source database, be sure to fix them before you create the dump file. The workflow does not have the ability to diagnose or remediate problems in the database.

Sample Scenarios

This topic shows you how to use various parameters to achieve the following database refresh scenarios in your environment using the ["Load Sybase Database Dump"](#) workflow:

Scenario 1: Database Dump File is Not Encrypted or Striped

This is the simplest Sybase ASE database refresh scenario. It does not matter whether the database dump file is compressed – if decompression is required, it is handled automatically by the workflow prior to the refresh.

Parameter Name	Example Value	Description
Call Wrapper	jython	Command that will be used to construct the call wrapper. The workflow uses the call wrapper to execute subsequent steps as either the OS administrative user (for example: <code>sudo su - root /opt/hp/dma/client/bin/jython.sh</code>) or the owner of the Sybase ASE installation (for example: <code>sudo su - sybase /opt/hp/dma/client/bin/jython.sh</code>).
Sybase OS User Name	sybase	OS user (typically, sybase) who owns the Sybase ASE installation directory.
Dump File List	/var/tmp/mytestdb.dmp	Comma-separated list of database dump files (with absolute paths—all specified paths must exist). For a single dump file, no comma is necessary.

Be sure that the default values for all remaining parameters are appropriate for your environment (see ["Parameters for Load Sybase Database Dump" on page 751](#)).

Scenario 2: Database Dump File is Encrypted

This scenario requires you to specify the encryption password for the database dump file. It does not matter whether the database dump file is compressed – if decompression is required, it is handled automatically by the workflow prior to the refresh.

Parameter Name	Example Value	Description
Call Wrapper	jython	Command that will be used to construct the call wrapper. The workflow uses the call wrapper to execute subsequent steps as either the OS administrative user (for example: <code>sudo su - root /opt/hp/dma/client/bin/jython.sh</code>) or the owner of the Sybase ASE installation (for example: <code>sudo su - sybase /opt/hp/dma/client/bin/jython.sh</code>).
Sybase OS User Name	sybase	OS user (typically, sybase) who owns the Sybase ASE installation directory.
Dump File List	/var/tmp/mytestdb.dmp	Comma-separated list of database dump files (with absolute paths—all specified paths must exist). For a single dump file, no comma is necessary.
Dump File Password	MyPassword1@#	Password required to decrypt a password-protected encrypted database dump file (required if the dump file is encrypted). Note: You cannot use an encrypted dump file to perform a cross-platform refresh when an architectural endian difference exists (for example: create dump on Linux, load dump on Solaris).

Be sure that the default values for all remaining parameters are appropriate for your environment (see ["Parameters for Load Sybase Database Dump" on page 751](#)).

Scenario 3: Database Dump File is Striped

In this scenario, the database dump file has been striped across multiple files. You must specify all the individual stripe files in the Dump File List parameter (separate them with commas).

If the stripe files are encrypted, you must specify the Dump File Password parameter.

It does not matter whether the database dump file is compressed – if decompression is required, it is handled automatically by the workflow prior to the refresh.

Parameter Name	Example Value	Description
Call Wrapper	jython	Command that will be used to construct the call wrapper. The workflow uses the call wrapper to execute subsequent steps as either the OS administrative user (for example: <code>sudo su - root</code> <code>/opt/hp/dma/client/bin/jython.sh</code>) or the owner of the Sybase ASE installation (for example: <code>sudo su - sybase</code> <code>/opt/hp/dma/client/bin/jython.sh</code>).
Sybase OS User Name	sybase	OS user (typically, sybase) who owns the Sybase ASE installation directory.
Dump File List	<code>/var/tmp/mytestdb1.dmp,</code> <code>/var/tmp/mytestdb2.dmp,</code> <code>/var/tmp/mytestdb3.dmp</code>	Comma-separated list of database dump files (with absolute paths—all specified paths must exist). For a single dump file, no comma is necessary.
Dump File Password	MyPassword1@#	Password required to decrypt a password-protected encrypted database dump file (required if the dump file is encrypted). Note: You cannot use an encrypted dump file to perform a cross-platform refresh when an architectural endian difference exists (for example: create dump on Linux, load dump on Solaris).

Be sure that the default values for all remaining parameters are appropriate for your environment (see ["Parameters for Load Sybase Database Dump" on page 751](#)).

Scenario 4: Using a Cache Dump File

In this scenario, the database dump file has an associated cache dump file. You must specify the name of the cache dump file by using the Cache Dump File parameter. The workflow will rebuild and bind the cache after the database dump file is loaded into the target database.

If the database dump file is encrypted, you must specify the Dump File Password parameter.

If the cache dump file is encrypted, you must specify the Cache Dump File Password parameter.

Parameter Name	Example Value	Description
Call Wrapper	jython	Command that will be used to construct the call wrapper. The workflow uses the call wrapper to execute subsequent steps as either the OS administrative user (for example: <code>sudo su - root /opt/hp/dma/client/bin/jython.sh</code>) or the owner of the Sybase ASE installation (for example: <code>sudo su - sybase /opt/hp/dma/client/bin/jython.sh</code>).
Sybase OS User Name	sybase	OS user (typically, sybase) who owns the Sybase ASE installation directory.
Dump File List	/var/tmp/mytestdb.dmp	Comma-separated list of database dump files (with absolute paths—all specified paths must exist). For a single dump file, no comma is necessary.
Dump File Password	MyPassword1@#	Password required to decrypt a password-protected encrypted database dump file (required if the dump file is encrypted). Note: You cannot use an encrypted dump file to perform a cross-platform refresh when an architectural endian difference exists (for example: create dump on Linux, load dump on Solaris).
Cache Dump File	/var/tmp/runcache_mytestdb.txt	Database cache file associated with this database dump. This is a single filename (with absolute path—the path and file must exist). The file contains detailed information about any specific (non-default) data caches used by the source database and any database objects bound to those caches.

Be sure that the default values for all remaining parameters are appropriate for your environment (see ["Parameters for Load Sybase Database Dump" on page 751](#)).

How to Run this Workflow

This topic explains how to customize and run the ["Load Sybase Database Dump"](#) workflow in your environment.

Note: Prior to running this workflow, review the ["Prerequisites for this Workflow"](#), and ensure that all requirements are satisfied.

To customize and run the Load Sybase Database Dump workflow:

1. Create a deployable copy of the workflow.
2. Determine the values that you will specify for the following parameters. This is the minimum set of parameters required to run this workflow.

Parameter Name	Default Value	Description
Call Wrapper	jython	Command that will be used to construct the call wrapper. The workflow uses the call wrapper to execute subsequent steps as either the OS administrative user (for example: <code>sudo su - root /opt/hp/dma/client/bin/jython.sh</code>) or the owner of the Sybase ASE installation (for example: <code>sudo su - sybase /opt/hp/dma/client/bin/jython.sh</code>).
Sybase OS User Name	sybase	OS user (typically, sybase) who owns the Sybase ASE installation directory.
Dump File List	/var/tmp/dump.dmp	Comma-separated list of database dump files (with absolute paths—all specified paths must exist). For a single dump file, no comma is necessary.
Dump File Password	no default	Password required to decrypt a password-protected encrypted database dump file (required if the dump file is encrypted). Note: You cannot use an encrypted dump file to perform a cross-platform refresh when an architectural endian difference exists (for example: create dump on Linux, load dump on Solaris).

Note: This is the minimum set of parameters required to run this workflow. You may need to expose additional parameters depending on your objectives.

See ["Parameters for Load Sybase Database Dump" on page 751](#) for detailed descriptions of all input parameters for this workflow, including default values.

To avoid having to re-enter passwords whenever they change, you can create a policy to

provide them to the workflow.

3.
 - a. In the workflow editor, expose any additional parameters that you need (see [How to Expose Additional Workflow Parameters](#) on page 70). You will specify values for those parameters when you create the deployment.
 - b. Save the changes to the workflow (click **Save** in the lower right corner).
 - c. Create a new deployment.
 - d. On the **Parameters** tab, specify values for the required parameters listed in step 2 and any additional parameters that you have exposed. You do not need to specify values for those parameters whose default values are appropriate for your environment.
 - e. On the **Targets** tab, specify one or more targets for this deployment.
 - f. Save the deployment (click **Save** in the lower right corner).
 - g. Run the workflow using this deployment.
4. The workflow will complete and report “Success” on the Console if it has run successfully. If an invalid parameter value is specified, an error is logged, and the workflow terminates in the “Failure” state.

Parameters for Load Sybase Database Dump

The following tables describe the required and optional input parameters for this workflow. Most of these parameters are not initially visible in a deployment. For most parameters, if you do not specify a value for a parameter, a default value is assigned in the following steps:

- Gather Parameters for Sybase Dump or Load
- Gather Advanced Parameters for Sybase Database Load

Input Parameters for the Load Sybase Database Dump Workflow

Parameter Name	Default Value	Required	Description
ASE SysAdmin Password	password	required	Password for the Sybase ASE user specified in the ASE SysAdmin Username parameter.
ASE SysAdmin Username	sa	required	The Sybase ASE user who can perform all administrative operations (typically sa). This user will perform the database load operation.
Cache Dump File	no default	optional	Database cache file associated with this database dump. This is a single filename (with absolute path—the path and file must exist). The file contains detailed information about any specific (non-default) data caches used by the source database and any database objects bound to those caches.
Call Wrapper	jython	required	Command that will be used to construct the call wrapper. The workflow uses the call wrapper to execute subsequent steps as either the OS administrative user (for example: <code>sudo su - root /opt/hp/dma/client/bin/jython.sh</code>) or the owner of the Sybase ASE installation (for example: <code>sudo su - sybase /opt/hp/dma/client/bin/jython.sh</code>).
DBCC Checks	checkdb, checkalloc, checkcatalog	optional	List of database consistency checker (DBCC) checks that you want to run to ensure that there are no problems with the database after the dump file is loaded.
DBCC Error Directory	/var/tmp	optional	The directory (with absolute path) where you want to store the DBCC results (output files) for post-load checks. This directory must exist.
Database Instance Name	NY_DS	required	The name of the Sybase ASE instance where the database will be loaded from the dump file (or files).
Dump Device Name	n/a	n/a	Not used in this release.

Input Parameters for the Load Sybase Database Dump Workflow, continued

Parameter Name	Default Value	Required	Description
Dump File List	/var/tmp/dump.dmp	required	Comma-separated list of database dump files (with absolute paths—all specified paths must exist). For a single dump file, no comma is necessary.
Dump File Password	no default	optional	Password required to decrypt a password-protected encrypted database dump file (required if the dump file is encrypted). Note: You cannot use an encrypted dump file to perform a cross-platform refresh when an architectural endian difference exists (for example: create dump on Linux, load dump on Solaris).
Dump File Path	n/a	n/a	Not used in this release.
Local Backup Instance Name	n/a	n/a	Not used in this release.
Local Backup Instance Port	n/a	n/a	Not used in this release.
Remote Backup Instance Name	n/a	n/a	Not used in this release.
Remote Backup Instance Port	n/a	n/a	Not used in this release.
Sybase ASE Home Directory	/home/sybase/ASE_15	required	Sybase ASE installation home directory, where the destination database resides. Sybase ASE will examine the interface file that exists in this directory to determine where to load the specified database dump file (or files).
Sybase OS User Name	sybase	required	OS user (typically, sybase) who owns the Sybase ASE installation directory.
Target Database Instance Name	NY_DS	required	Name of the Sybase ASE instance where the dump file (or files) will be loaded.
Target Database Name	mytestdb	required	Name of the database where the dump file (or files) will be loaded.

Input Parameters for the Load Sybase Database Dump Workflow, continued

Parameter Name	Default Value	Required	Description
Target Database Page Size	4 KB	optional	Page size of the target database server (in kilobytes).

Dump And Load Sybase Database

This workflow enables you to dump the contents of a Sybase ASE database (the **source**) into a file (the database dump file) and load the contents of that file into an existing Sybase ASE database (the **destination**).

The workflow performs extensive validation checks prior to and immediately after the dump operation at the source to ensure that the dump file is valid. It also performs validation checks prior to and immediately after the load operation at the destination to ensure that the data was successfully loaded.

This workflow can perform a cross-platform database refresh (dump and load) when necessary. After it performs a cross-platform load operation, the workflow rebuilds the indexes (clustered or non-clustered indexes on APL/DOL tables) to avoid page linkage or index corruption issues. Password protected dump cannot be supported for cross platform dump and load.

If any source database objects are bound to a specific (non-default) cache, the workflow will create a cache dump file—provided that you specify a valid value for the Cache Dump File parameter. The cache dump file contains details about the specific caches used by the source database and any objects that are bound to each cache. This file is in data-readable format. The workflow uses the cache dump file to refresh the destination database cache (provided that ample cache space is available). The workflow cannot, however, configure or enable cache buffering.

This workflow can create and load database dump files that are striped, compressed (at any level 1-9), encrypted, or any combination thereof.

To use this workflow in your environment, see the following information:

Topic	Information Included
"Prerequisites for this Workflow"	List of prerequisites that must be satisfied before you can run this workflow
"How this Workflow Works"	Information about what the workflow does, including validation checks performed, steps executed, and a high-level process flow
"How to Run this Workflow"	Instructions for running this workflow in your environment
"Sample Scenarios"	Examples of typical parameter values for this workflow
"Parameters for Dump and Load Sybase Database"	List of input parameters for this workflow

The process of deploying and running this workflow is the same for all scenarios, but the parameters required will differ depending on the specific scenario that you are implementing.

The workflow provides default values for most parameters. These default values are usually sufficient for a "typical" database refresh. You can override the defaults by specifying parameter values in the

deployment. You can also expose additional parameters in the workflow, if necessary, to accomplish more advanced scenarios.

Any parameters not explicitly specified in the deployment will have the default values listed in ["Parameters for Dump and Load Sybase Database" on page 769](#).

Note: To view detailed information about the steps included in this workflow, see [Steps in this Workflow](#).

Prerequisites for this Workflow

Caution: You cannot perform a database dump if there are dependencies between the source database and another database in the same or a different Sybase ASE instance. You must remove or disable object referencing (for example: triggers, views, stored procedures, etc.) before you run this workflow.

The following prerequisites must be satisfied before you can run the Dump and Load Sybase Database workflow:

1. The **source** and **destination** databases must exist before the workflow runs.
2. The source and destination databases must NOT be mounted on the master device.
3. The source and destination database servers must use the same page size.
4. No database users may be logged in to the destination database server when this workflow runs.
5. The source Adaptive Server instance that executes the `dump` command and the local source Backup Server instance must both be running, and they must be able to communicate with each other.
6. The destination Adaptive Server instance that executes the `load` command and the local destination Backup Server instance must both be running, and they must be able to communicate with each other.
7. The master database system table (`sys.servers`) for both source and destination must contain an entry that assigns the local Backup Server instance to `SYB_BACKUP`.
8. By default, the workflow will create the database dump file with the following file name format:

`dump_file_path/databasename_datetime.dmp`

For example: `/var/tmp/mytestdb_2012111283762.dmp`

9. If you specify a non-default file name (or names) in the Dump File List parameter, the path to each specified file must exist.

You must specify an operating system file in the Dump File List parameter (for example: `/var/temp/mydbdump.dmp`). You cannot specify a dump device.

The database dump file must be accessible from the server where the workflow is executed. The file must be available on the local machine or via a Network File System (NFS) mount.

The workflows currently do not support writing or reading the database dump file from tape devices.

10. Adequate disk space must be available on the shared NFS location where the dump file will be stored.
11. On Linux and Solaris platforms, the `sudo` package must be installed on the target servers.
12. The workflow assumes the following for both the source and destination:
 - The Adaptive Server component is installed under `/home/Sybase/ASE_15`
 - The Adaptive Server instance name is `NY_DS`
 - The database name is `mytestdb`
 - The database dump file is stored in the `/var/tmp` directory
 - `/var/tmp` is an NFS mount point.
 - The Sybase ASE user specified in the ASE SysAdmin Username parameter is permitted to access the `/var/tmp` directory.
 - The user specified in the Sybase OS User Name parameter (sybase by default) must own the installation directory and be a member of the "sybase" group.

Note: The workflow currently does not support reading the database dump file from tape devices.

Note: This workflow does not support dump file password encryption for **cross-platform** database refresh (for example: the database dump file was created on a Linux server, and you are loading it onto a Solaris server).

Additional Considerations

It is good practice to run basic database consistency checks (DBCCs) on the source database before running this workflow. You can do this by creating a simple workflow that includes the Run Sybase DBCC Checks step included in this solution pack.

If database transactions occur on the source database after the dump file is created, you should apply the latest transaction log dump to the destination database after you run the "[Load Sybase Database Dump](#)" workflow. Otherwise, these transactions will be missing from the destination database.

For information about prerequisites for Sybase ASE, refer to the [Sybase ASE Product Documentation](#).

How this Workflow Works

This topic contains information about the ["Dump And Load Sybase Database"](#) workflow:

Caution: You cannot perform a database dump if there are dependencies between the source database and another database in the same or a different Sybase ASE instance. You must remove or disable object referencing (for example: triggers, views, stored procedures, etc.) before you run this workflow.

Validation Checks Performed

The workflow checks the following things prior to refreshing the database. If any of these checks fails, the workflow fails.

1. All required parameters have values. If any required parameter does not have a value—either a value that you specify or a default value—the workflow fails in the Sybase - Validate Database Dump Settings step.
2. The Sybase ASE software is installed.
3. The source database exists in the specified Sybase ASE instance and is online.
4. The source Adaptive Server and Backup Server components are running and able to communicate with each other so that they can perform the database dump.
5. Adequate disk space is available to store the database dump file.
6. The destination database exists in the specified Sybase ASE instance and is online.
7. The destination Adaptive Server and Backup Server components are running and able to communicate with each other.
8. The destination database server page size matches the source database server page size.
9. The Sybase ASE version of the source database is compatible with that of the destination database. The following versions are compatible:

Dump File Version	Target Instance Version
Sybase ASE 15.0.3 or 15.5	Sybase ASE 15.0.3 or 15.5
Sybase ASE 12.5.4	Sybase ASE 15.0.3

10. The size of the destination database is sufficient to load the database dump file created from the source database.

The workflow then determines whether the destination database is currently in use by Sybase ASE users. If the database is in use, the workflow creates a backup of the destination database users and groups in `tempdb` before it loads the contents of the dump file. It restores the users after the database is refreshed.

Steps Executed

The "Dump And Load Sybase Database" workflow includes the following steps. Each step must complete successfully before the next step can start. If a step fails, the workflow reports a failure, and all subsequent steps are skipped.

Process Flow

This workflow performs the following tasks:

1. Creates the Instance Wrapper and Server Wrapper.
2. Verifies that the DMA server is able to communicate with the server where the workflow is running.
3. Performs the pre-dump [validation checks](#) described above.
4. Generates the cache descriptor file for the source database. This is used to replicate the cache objects on the destination server.
5. Performs the database dump operation to create the database dump file.
6. Performs post-dump validation checks to ensure that all required parameters had valid values.
7. Reads the header of the database dump file, and validates that the source Sybase ASE page size matches the target Sybase ASE page size. The workflow fails if the page sizes do not match.
8. Backs up any existing database users and groups.
9. Determines whether the source and destination database servers have different byte architectures (big-endian versus little-endian).
10. Enables the database level “dbo use only” option to ensure that no users except the database owner are accessing the destination database.
11. Loads the database dump file on the destination database server, and refreshes the destination database.
12. Brings the destination database online and performs the post-refresh checks.
13. Rebuild the indexes using the Sybase ASE recommended `sp_post_xpload` system stored procedure.
14. Runs the specified database consistency checker (DBCC) checks to ensure that no database tables or objects have become corrupted. The output of these checks is printed in the step log and stored in files under the specified directory.
15. Builds the specified cache (if specified), and binds the database object to either the default data cache or the specified cache.

Tips and Best Practices

It is good practice to run basic database consistency checks (DBCCs) on the source database before running this workflow to ensure that there are no internal errors in the database. You can do this by creating a simple workflow that includes the Run Sybase DBCC Checks step included in this solution pack.

If you find errors in the source database, be sure to fix them before running this workflow. The workflow does not have the ability to diagnose or remediate problems in the database prior to performing the database dump.

Sample Scenarios

This topic shows you how to use various parameters to achieve the following database refresh scenarios in your environment using the ["Dump And Load Sybase Database"](#) workflow:

Scenario 1: Perform a Database Refresh Using a Dump File is Not Encrypted or Striped

This is the simplest Sybase ASE database refresh scenario.

Parameter Name	Example Value	Description
Call Wrapper	jython	Command that will be used to construct the call wrapper. The workflow uses the call wrapper to execute subsequent steps as either the OS administrative user (for example: <code>sudo su - root /opt/hp/dma/client/bin/jython.sh</code>) or the owner of the Sybase ASE installation (for example: <code>sudo su - sybase /opt/hp/dma/client/bin/jython.sh</code>).
Sybase OS User Name	sybase	OS user (typically, sybase) who owns the Sybase ASE installation directory.
Dump File List	/var/tmp/mytestdb.dmp	Comma-separated list of database dump files (with absolute paths—all specified paths must exist). For a single dump file, no comma is necessary.

Be sure that the default values for all remaining parameters are appropriate for your environment (see [Parameters for Load Sybase Database Dump](#)).

Scenario 2: Perform a Database Refresh Using a Dump File that is Compressed and Encrypted

This scenario requires you to specify the encryption password and compression level for the database dump file.

Parameter Name	Example Value	Description
Call Wrapper	jython	Command that will be used to construct the call wrapper. The workflow uses the call wrapper to execute subsequent steps as either the OS administrative user (for example: <code>sudo su - root /opt/hp/dma/client/bin/jython.sh</code>) or the owner of the Sybase ASE installation (for example: <code>sudo su - sybase /opt/hp/dma/client/bin/jython.sh</code>).
Sybase OS User Name	sybase	OS user (typically, sybase) who owns the Sybase ASE installation directory.
Dump File List	/var/tmp/mytestdb.dmp	Comma-separated list of database dump files (with absolute paths—all specified paths must exist). For a single dump file, no comma is necessary.
Dump File Compression Level	8	Compression level (1-9) to apply to the dump file (or files) that will be created.
Dump File Password	MyPassword1@#	Password required to encrypt and decrypt the database dump file. Note: You cannot use an encrypted dump file to perform a cross-platform refresh when an architectural endian difference exists (for example: create dump on Linux, load dump on Solaris).

Be sure that the default values for all remaining parameters are appropriate for your environment (see Parameters for Load Sybase Database Dump).

Scenario 3: Perform a Database Refresh Using a Dump File that is Striped

In this scenario, the database dump file will be striped across multiple files. You must specify all the individual stripe files in the Dump File List parameter (separate them with commas). If the stripe files are encrypted, you must also specify the Dump File Password parameter.

Parameter Name	Example Value	Description
Call Wrapper	jython	Command that will be used to construct the call wrapper. The workflow uses the call wrapper to execute subsequent steps as either the OS administrative user (for example: <code>sudo su - root /opt/hp/dma/client/bin/jython.sh</code>) or the owner of the Sybase ASE installation (for example: <code>sudo su - sybase /opt/hp/dma/client/bin/jython.sh</code>).
Sybase OS User Name	sybase	OS user (typically, sybase) who owns the Sybase ASE installation directory.
Dump File List	<code>/var/tmp/mytestdb1.dmp, /var/tmp/mytestdb2.dmp, /var/tmp/mytestdb3.dmp</code>	Comma-separated list of database dump files (with absolute paths—all specified paths must exist). For a single dump file, no comma is necessary.
Dump File Password	MyPassword1@#	Password required to encrypt and decrypt the database dump file. Note: You cannot use an encrypted dump file to perform a cross-platform refresh when an architectural endian difference exists (for example: create dump on Linux, load dump on Solaris).

Be sure that the default values for all remaining parameters are appropriate for your environment (see Parameters for Load Sybase Database Dump).

Scenario 4: Perform a Database Refresh Using a Cache Dump File

In this scenario, the database dump file has an associated cache dump file. You must specify the name of the cache dump file by using the Cache File parameter. The workflow will rebuild and bind the cache after the database dump file is loaded into the target database.

If the database dump file is encrypted, you must specify the Dump File Password parameter.

If the cache dump file is encrypted, you must specify the Cache Dump File Password parameter.

Parameter Name	Example Value	Description
Call Wrapper	jython	Command that will be used to construct the call wrapper. The workflow uses the call wrapper to execute subsequent steps as either the OS administrative user (for example: <code>sudo su - root /opt/hp/dma/client/bin/jython.sh</code>) or the owner of the Sybase ASE installation (for example: <code>sudo su - sybase /opt/hp/dma/client/bin/jython.sh</code>).
Sybase OS User Name	sybase	OS user (typically, sybase) who owns the Sybase ASE installation directory.
Dump File List	/var/tmp/mytestdb.dmp	Comma-separated list of database dump files (with absolute paths—all specified paths must exist). For a single dump file, no comma is necessary.
Dump File Password	MyPassword1@#	Password required to encrypt and decrypt the database dump file. Note: You cannot use an encrypted dump file to perform a cross-platform refresh when an architectural endian difference exists (for example: create dump on Linux, load dump on Solaris).
Cache File	/var/tmp/runcache_mytestdb.txt	Database cache file associated with this database dump. This is a single filename (with absolute path—path must exist). The file contains detailed information about any specific (non-default) data caches used by the source database and any database objects bound to those caches.

Be sure that the default values for all remaining parameters are appropriate for your environment (see Parameters for Load Sybase Database Dump).

How to Run this Workflow

This topic explains how to customize and run the ["Dump And Load Sybase Database"](#) workflow in your environment.

Note: Prior to running this workflow, review the ["Prerequisites for this Workflow"](#), and ensure that all requirements are satisfied.

To customize and run the Dump and Load Sybase Database workflow:

1. Create a deployable copy of the workflow.
2. Determine the values that you will specify for the following parameters. This is the minimum set of parameters required to run this workflow.

Parameter Name	Default Value	Description
Call Wrapper	jython	Command that will be used to construct the call wrapper. The workflow uses the call wrapper to execute subsequent steps as either the OS administrative user (for example: <code>sudo su - root /opt/hp/dma/client/bin/jython.sh</code>) or the owner of the Sybase ASE installation (for example: <code>sudo su - sybase /opt/hp/dma/client/bin/jython.sh</code>).
Sybase OS User Name	sybase	OS user (typically, sybase) who owns the Sybase ASE installation directory.
Cache File	no default	Database cache file associated with this database dump. This is a single filename (with absolute path—path must exist). The file contains detailed information about any specific (non-default) data caches used by the source database and any database objects bound to those caches.
Dump File Compression Level	7	Compression level (1-9) to apply to the dump file (or files) that will be created.
Dump File Password	no default	Password required to encrypt and decrypt the database dump file. Note: You cannot use an encrypted dump file to perform a cross-platform refresh when an architectural endian difference exists (for example: create dump on Linux, load dump on Solaris).
Sybase ASE Home Directory	/home/sybase/ASE_15	Sybase ASE installation home directory, where the destination database resides. Sybase ASE will examine the interface file that exists in this directory to determine where to load the specified database dump file (or files).

Parameter Name	Default Value	Description
		If the Sybase ASE installation home directory is the same on the source and the destination servers, you do not need to specify this parameter. The default is assumed for the source—if you want to specify a different home directory for the source, you will need to expose the Sybase ASE Home Directory parameter in the Gather Advanced Parameters for Sybase Database Dump step (see step 3).

Note: This is the minimum set of parameters required to run this workflow. You may need to expose additional parameters depending on your objectives.

See ["Parameters for Load Sybase Database Dump" on page 751](#) for detailed descriptions of all input parameters for this workflow, including default values.

- In the workflow editor, expose any additional parameters that you need. You will specify values for these parameters when you create the deployment.
- Save the changes to the workflow (click **Save** in the lower right corner).
- Create a new deployment.
 - On the Targets tab, select all the target servers—both source and destination—that will participate in this database refresh. The targets that you select here will be available in the Target Parameters drop-down menus on the Run page (see [step 7](#)).
 - On the Parameters tab, specify values for the required parameters listed in [step 2](#) and any additional parameters that you exposed in [step 3](#). You do not need to specify values for those parameters whose default values are appropriate for your environment.
- Save the deployment (click **Save** in the lower right corner).
- Run the workflow using this deployment.

On the Run page, select the following targets from the respective drop-down menus:

Parameter Name	Default	Description
Source Instance	no default	<p>The Adaptive Server instance where the dump file will be created. You specify this when you run the workflow.</p> <p>Note: The Source Instance that you specify at run time must match the Source Database Instance Name that you specify in the deployment.</p>
Target Instance	no default	The Adaptive Server instance where the destination database will be loaded from the dump file (or files). You specify this when you run the

Parameter Name	Default	Description
		<p>workflow.</p> <p>Note: The Target Instance that you specify at run time must match the Target Database Instance Name that you specify in the deployment.</p>

The workflow will complete and report “Success” on the Console if it has run successfully. If an invalid parameter value is specified, an error is logged, and the workflow terminates in the “Failure” state.

Parameters for Dump and Load Sybase Database

The following tables describe the required and optional input parameters for this workflow. Most of these parameters are not initially visible in a deployment. For most parameters, if you do not specify a value for a parameter, a default value is assigned in the following steps:

- Gather Parameters for Sybase Dump or Load
- Gather Advanced Parameters for Sybase Database Dump

Input Parameters for the Dump Sybase Database Workflow

Parameter Name	Default Value	Required	Description
ASE SysAdmin Password	password	required	Password for the Sybase ASE user specified in the ASE SysAdmin Username parameter.
ASE SysAdmin Username	sa	required	The Sybase ASE user who can perform all administrative operations (typically sa). This user will perform the database dump and load operations.
Cache Dump File	no default	optional	Database cache file associated with this database dump. This is a single filename (with absolute path—path must exist). The file contains detailed information about any specific (non-default) data caches used by the source database and any database objects bound to those caches.
Call Wrapper	jython	required	Command that will be used to construct the call wrapper. The workflow uses the call wrapper to execute subsequent steps as either the OS administrative user (for example: <code>sudo su - root /opt/hp/dma/client/bin/jython.sh</code>) or the owner of the Sybase ASE installation (for example: <code>sudo su - sybase /opt/hp/dma/client/bin/jython.sh</code>).
DBCC Checks	checkdb, checkalloc, checkcatalog	optional	List of database consistency checker (DBCC) checks that you want to run to ensure that there are no problems with the database after the dump file is loaded.
DBCC Error Directory	/var/tmp	optional	The directory (with absolute path) where you want to store the DBCC results (output files) for post-load checks. This directory must exist.
Dump Device Name	n/a	n/a	Not used in this release.
Dump File Compression Level	7	optional	Compression level (1-9) to apply to the dump file (or files) that will be created.

Input Parameters for the Dump Sybase Database Workflow, continued

Parameter Name	Default Value	Required	Description
Dump File List	<code>/var/tmp/<dbname>_<datetime>.dmp</code> For example: <code>/var/tmp/mytestdb_2012111283762.dmp</code> If you specify a non-default file name (or names) in the Dump File List parameter, the path to each specified file must exist.	required	Comma-separated list of database dump files (with absolute paths—all specified paths must exist). For a single dump file, no comma is necessary.
Dump File Password	no default	optional	Password required to encrypt and decrypt the database dump file. Note: You cannot use an encrypted dump file to perform a cross-platform refresh when an architectural endian difference exists (for example: create dump on Linux, load dump on Solaris).
Dump File Path	n/a	n/a	Not used in this release.
Local Backup Instance Name	n/a	n/a	Not used in this release.
Local Backup Instance Port	n/a	n/a	Not used in this release.
Remote Backup Instance Name	n/a	n/a	Not used in this release.
Remote Backup Instance Port	n/a	n/a	Not used in this release.
Role Password SQL Statement	no default	required	Not used in this release.
Source Database Instance Name	NY_DS	required	Name of the Adaptive Server instance where the dump file (or files) will be created. You specify the value of this parameter in the deployment.

Input Parameters for the Dump Sybase Database Workflow, continued

Parameter Name	Default Value	Required	Description
			Note: The Source Instance that you specify at run time must match the Source Database Instance Name that you specify in the deployment.
Source Database Name	mytestdb	required	Name of database from which the dump file (or files) will be created.
Source Instance	no default	required	<p>The Adaptive Server instance where the dump file will be created. You specify this when you run the workflow.</p> <p>Note: The Source Instance that you specify at run time must match the Source Database Instance Name that you specify in the deployment.</p>
Sybase ASE Home Directory	/home/sybase/ASE_15	required	Sybase ASE installation home directory, where the source and destination databases each reside. Sybase ASE will examine the interface file that exists in this directory to determine where to first create and then load the specified database dump file (or files).
Sybase OS User Name	sybase	required	OS user (typically, sybase) who owns the Sybase ASE installation directory.
Target Database Instance Name	NY_DS	required	<p>Name of the Adaptive Server instance where the destination database will be loaded from the dump file (or files). You specify the value of this parameter in the deployment.</p> <p>Note: The Target Instance that you specify at run time must match the Target Database Instance Name that you specify in the deployment.</p>
Target Database Name	mytestdb	required	Name of the database where the dump file (or files) will be loaded.
Target Instance	no default	required	<p>The Adaptive Server instance where the destination database will be loaded from the dump file (or files). You specify this when you run the workflow.</p> <p>Note: The Target Instance that you specify at run time must match the Target Database Instance Name that you specify in the deployment.</p>

Sybase - Start or Stop Instance

The Sybase - Start or Stop Instance workflow starts or stops an existing Sybase instance (data server and backup server).

To use this workflow in your environment, see the following information:

Topic	Information Included
"Prerequisites for this Workflow" on the next page	List of prerequisites that must be satisfied before you can run this workflow
"How this Workflow Works" on page 774	Information about what the workflow does, including validation checks performed, steps executed, and step descriptions
" How to Run this Workflow" on page 775	Instructions for running this workflow in your environment
"Parameters for Sybase - Start or Stop Instance" on page 777	List of input parameters for this workflow

Prerequisites for this Workflow

Be sure that the following prerequisites are satisfied before you run the MySQL - Start or Stop workflow:

- This solution requires DMA version 10.50.001.000 (or later).

The latest DMA solution packs require the latest DMA platform. To use the latest solution packs, update the DMA platform. DMA10.50.001.000 solution packs are supported on DMA10.50.001.000 (and later).

- You have installed the Database Provisioning solution pack.
- Instance that is going to be started or stopped needs to be discovered before running this workflow.

The information presented here assumes the following:

- DMA is installed and operational.
- At least one suitable target server (database) is available.
- You are logged in to the DMA web interface.
- You have permission to create, edit, and deploy copies of the workflows included in this solution pack.

For more information about prerequisites for MySQL database, refer to the [Sybase Product Documentation](#).

How this Workflow Works

This workflow performs the following actions:

- Starts or stops an existing Sybase instance.

Steps Executed by the Workflow

The Sybase - Start or Stop Instance workflow includes the following steps. Each step must complete successfully before the next step can start. If a step fails, the workflow reports a failure and all subsequent steps are skipped.

Steps Used by Sybase - Start or Stop Instance

Workflow Step	Description
Gather Parameters for Sybase Start or Stop Instance	This step gathers the parameters needed for starting or stopping a Sybase instance.
Gather Advanced Parameters for Sybase Start or Stop Instance	This step gathers advanced parameters for starting or stopping a Sybase instance.
Validate Parameters for Sybase Start or Stop Instance	This step validates the parameters for Sybase - Start or Stop Instance workflow.
Verify Status of Sybase Instance	Verifies the status of instance by checking if data server and backup server are running or not.
Startup Sybase Servers v2	This step implements the Sybase commands to startup the Sybase servers. It can startup dataserver and backupserver if proper input parameter values are provided and also verifies that the servers have been started successfully by checking the process running on OS.
Shutdown Sybase Servers v3	Performs shutdown of the Sybase dataserver instance.
Verify Status of Sybase Instance	Verifies the status of instance by checking if data server and backup server are running or not.

How to Run this Workflow

The following instructions show you how to customize and run the Sybase - Start or Stop Instance workflow in your environment.

The workflow provides default values for some parameters. These default values are usually sufficient for a "typical" installation. You can override the defaults by specifying parameter values in the deployment. You can also expose additional parameters in the workflow, if necessary, to accomplish more advanced scenarios. Any parameters not explicitly specified in the deployment will have the default values listed in ["Parameters for Sybase - Start or Stop Instance" on page 777](#).

Note: Before following this procedure, review the ["Prerequisites for this Workflow" on page 773](#), and ensure that all requirements are satisfied.

To use the Sybase - Start or Stop Instance workflow:

1. Create a deployable copy of the workflow.
2. Determine the values that you will specify for the parameters.

Note: There are no mandatory parameters required to run this workflow. All parameters are optional. You may need to expose additional parameters depending on your objectives.
3. In the workflow editor, expose any additional parameters that you need. You will specify values for those parameters when you create the deployment or at runtime.
4. Save the changes to the workflow (click **Save** in the lower right corner).
5. Create a new deployment.
6. On the Parameters tab, specify values (or set the type to Runtime Value) for the required parameters listed in step 2 and any additional parameters that you have exposed. You do not need to specify values for those parameters whose default values are appropriate for your environment.
7. On the Targets tab, specify one or more targets for this deployment.
8. Save the deployment (click **Save** in the lower right corner).
9. Run the workflow using this deployment, specifying any runtime parameters.

To verify the results:

The workflow will complete and report SUCCESS on the Console if it has run successfully. If an error occurs during workflow execution, the error is logged, and the workflow terminates in the FAILURE state. The database will be removed from the DMA environment section upon SUCCESS as well.

Sample Scenario

This topic shows you typical parameter values for different use cases for the Sybase - Start or Stop Instance workflow.

Scenario 1: Start Sybase instance

Input Parameters for Sybase - Gather Parameters for Start or Stop Instance

Parameter Name	Example Value	Description
Action	Start	When set to "Start", the Sybase instance will be started.

Scenario 2: Stop Sybase instance

Input Parameters for Sybase - Gather Parameters for Start or Stop Instance

Parameter Name	Example Value	Description
Action	Stop	When set to "Stop", the Sybase instance will be stopped.

Note: Some of these parameters are not exposed by default in the deployment.

Be sure that the default values for all remaining input parameters are appropriate for your environment (see ["Parameters for Sybase - Start or Stop Instance" on the next page](#)).

Parameters for Sybase - Start or Stop Instance

The following tables describe the required and optional input parameters for this workflow.

Parameters Defined in this Step: Sybase - Gather Parameters for Start or Stop Instance

Parameter Name	Default Value	Required	Description
Action	no default	required	If set to "Start", the Sybase instance will be started. If set to "Stop", the Sybase instance will be stopped.

Parameters Defined in this Step: Sybase - Gather Advanced Parameters for Start or Stop Instance

Parameter Name	Default Value	Required	Description
Force Shutdown Server	False	optional if Action is set to "stop"	If set to "true", the Sybase instance will shutdown the server with no wait. If set to "False", the Sybase instance will shutdown normally.

Sybase Release Management

This workflow is designed to release **T-SQL** code for a Sybase Adaptive Server Enterprise (Sybase ASE) database. The workflow can be used to:

- Release **DDL/DML/DCL** T-SQL code.
- Update the database server level configuration.
- Update the database options.
- Restrict the user from executing prohibited commands or regular expressions in the code.

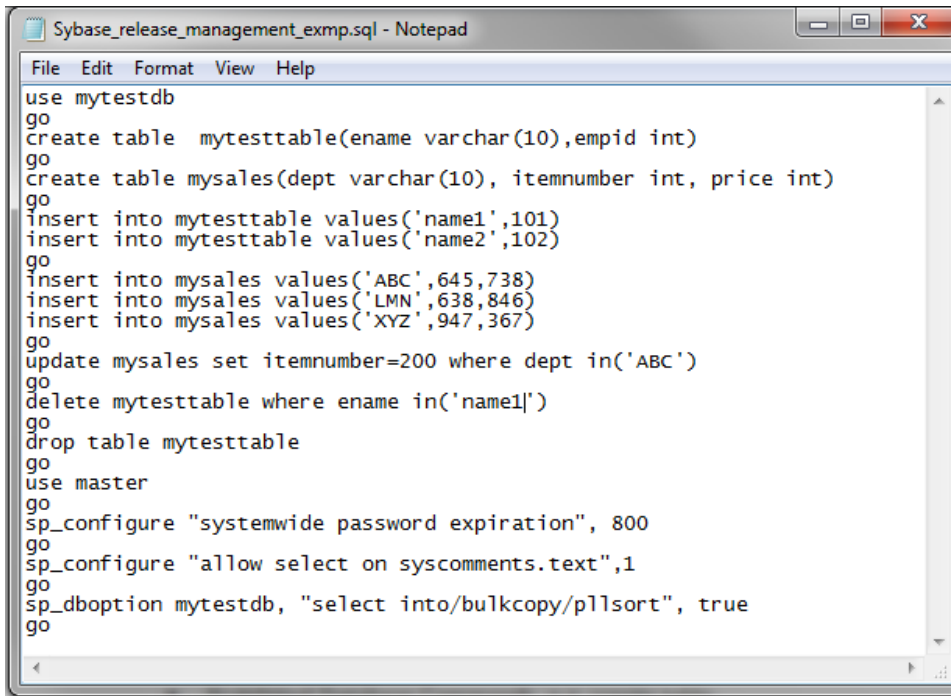
T-SQL scripts, Adaptive Server configuration parameters, and database options are deployed and executed against target Sybase ASE databases.

The workflow extensively checks the T-SQL scripts before executing and committing changes to the target database on the discovered ASE Server. It can match a regular expression and can prohibit restricted database commands (DDL/DML/DCL), server level configuration changes, and database level option settings. It also avoids executing any remote database commands such as creating proxy tables or proxy databases.

This workflow enables you to perform the following Sybase ASE database commands:

- DB DDL/DML/DCL—to run common Sybase ASE database queries
- `sp_dboption`—to control the database level configuration
- `sp_configure`—to control the server level configuration
- `regex`—to set exceptions to the regular expiration of permissions

Before running the Sybase Release Management workflow you need to create the SQL script file (or files), for example:



```

use mytestdb
go
create table mytesttable(ename varchar(10),empid int)
go
create table mysales(dept varchar(10), itemnumber int, price int)
go
insert into mytesttable values('name1',101)
insert into mytesttable values('name2',102)
go
insert into mysales values('ABC',645,738)
insert into mysales values('LMN',638,846)
insert into mysales values('XYZ',947,367)
go
update mysales set itemnumber=200 where dept in('ABC')
go
delete mytesttable where ename in('name1')
go
drop table mytesttable
go
use master
go
sp_configure "systemwide password expiration", 800
go
sp_configure "allow select on syscomments.text",1
go
sp_dboption mytestdb, "select into/bulkcopy/pllsort", true
go
  
```

You can use the input parameters to customize the following:

- Provide prohibited database commands (DDL/DML/DCL commands).
- Override the prohibited configuration updates (sp_configure commands) with a list of approved updates.
- Override the prohibited database options (sp_dboption commands) with a list of approved options.
- Provide prohibited regular expressions.
- Check the syntax of the SQL queries.
- Show the query plan—without actually executing the SQL scripts.
- Estimate the time required to execute the SQL scripts—without actually executing.
- Show the logical and physical input and output counts that will be required to execute each query—without actually executing.
- If all the tests pass, deploy and execute the SQL scripts against the target Sybase ASE databases.

Note: This workflow does not provide any rollback capability.

To use this workflow in your environment, see the following information:

Topic	Information Included
"Prerequisites for this Workflow"	List of prerequisites that must be satisfied before you can run this workflow
"How this Workflow Works"	Information about what the workflow does, including validation checks performed, and steps executed
"How to Run this Workflow"	Instructions for running this workflow in your environment
"Sample Scenarios"	Examples of typical parameter values for this workflow
Parameters	List of input parameters for this workflow

Prerequisites for this Workflow

Be sure that the following prerequisites are satisfied before you run the **"Sybase Release Management"** workflow.

Dependencies

- The latest DMA solution packs require the latest DMA platform. To use the latest solution packs, update the DMA platform. DMA 10.30 solution packs are supported on DMA 10.40 (and later).
- You have installed the Database Release Management solution pack.
- You have installed the native isql (Interactive SQL parser to Adaptive Server) utility from OCS (Open Client Server) and made it accessible via the user/password settings stored in the metadata. Check the Environment page for those settings.
- The user specified in the Sybase User parameter has default database access to the target database when logged in to Sybase ASE.
- The target database instance and the databases within it have been discovered prior to running this workflow to gather the instance information from the metadata.
- You need an SSO (System Security Officer) or SA (System Administrator) role to perform any server level or database level updates.
- The SQL script must reside in the software repository or on the target.

Supported Versions of Sybase ASE

15.0.3, 15.5, 15.7 (tested)

15.0, 15.0.1, 15.0.2 (not tested)

SQL Scripts

You need to create the SQL script file (or files) that manage the release. The files may contain the following Sybase ASE SQL commands:

- Supported DML, DDL, and DCL statements:

ALTER DATABASE	CREATE TABLE	REVOKE
ALTER ROLE	CREATE VIEW	SELECT
CHECKPOINT	DELETE	SELECT INTO
COMMIT	DISK INIT	SETUSER
CREATE CLUSTERED INDEX	DROP DATABASE	TRUNCATE
CREATE DATABASE	DROP INDEX	UPDATE
CREATE DEFAULTS	DROP SYNONYM	UPDATE ALL STATISTICS
CREATE NONCLUSTERED INDEX	DROP TABLE	UPDATE INDEX STATISTICS
CREATE ROLE	DROP VIEW	UPDATE STATISTICS
CREATE RULES	EXECUTE	UPDATE TABLE STATISTICS
CREATE SCHEMA	GRANT	
CREATE SYNONYM	INSERT	
	REORG REBUILD	

- All the Sybase system stored procedures, for example: sp_helpdb, sp_helpindex, sp_help
- All the global variable execution, for example: select @@version
- All the native Sybase system functions, for example: select db_name()
- All the Sybase supported dbcc commands, for example: dbcc checkalloc

Tip: List the SQL script files in the SQL scripts parameter in the order in which they need to be executed.

Sybase Adaptive Server Enterprise Documentation

For more information about prerequisites for "Sybase Release Management", refer to the [Sybase Adaptive Server Enterprise Documentation](#).

How this Workflow Works

The following information describes how the "Sybase Release Management" workflow works.

Overview

The workflow starts by constructing commands that will be used in subsequent steps and by gathering and validating input parameters.

If the T-SQL scripts, server level configurations, and database option settings do not exist on the specified target location, they are stored and downloaded from the DMA software repository.

Based on the parameters you set when you create your deployment, this workflow will do the following things:

- Scan the T-SQL code for prohibited database commands, prohibited configuration updates, prohibited database options, and regular expressions—if any are found, the workflow will exit with a failure code.
- Analyze the T-SQL code for remote server usage (database commands such as creating proxy tables or proxy databases)—if any are found, the workflow will exit with a failure code.
- Determine if there are syntax errors—if any problems are found, the query will not be executed, and the errors will be reported on the step log Error tab.
- Parse and verify that the server level configuration and database level options exist on the specified target database server and database respectively—if any are found, the workflow will exit with a failure code.
- Run the `isql` (Interactive SQL parser to Adaptive Server) utility to simulate the execution of the SQL script files—without running the actual T-SQL code. Based on your input parameters, show a query plan, show the statistics time, and/or show the statistics of logical/physical input and output. If you run this simulation, the workflow assumes that you want to review the reports so do not want to actually execute the SQL script files.
- Run the `isql` utility to deploy and execute the SQL script files against the target Sybase ASE databases—only if the run flag is set, no errors were found in the SQL scripts, and you did not request any of the simulation reports (Generate Query Plan, Generate Optimizer Statistics, or Generate Logical I/O Counts).

If the workflow proceeds successfully to the last step, it writes status messages to the Output tab of the step log. If it fails, it writes error messages to the Error tab.

Validation Checks Performed

This workflow validates the input parameters in the following ways:

1. Checks that there are values for the required input parameters: Sybase Home, Sybase User, Sybase Password, and SQL Scripts.
2. Checks whether the Sybase Release Management SQL scripts exist—if not, adds them to a list of files to be downloaded .
3. Checks that the database is online.
4. Checks that all flag parameters are y, yes, no, no, t, true, f, or false—case insensitive.

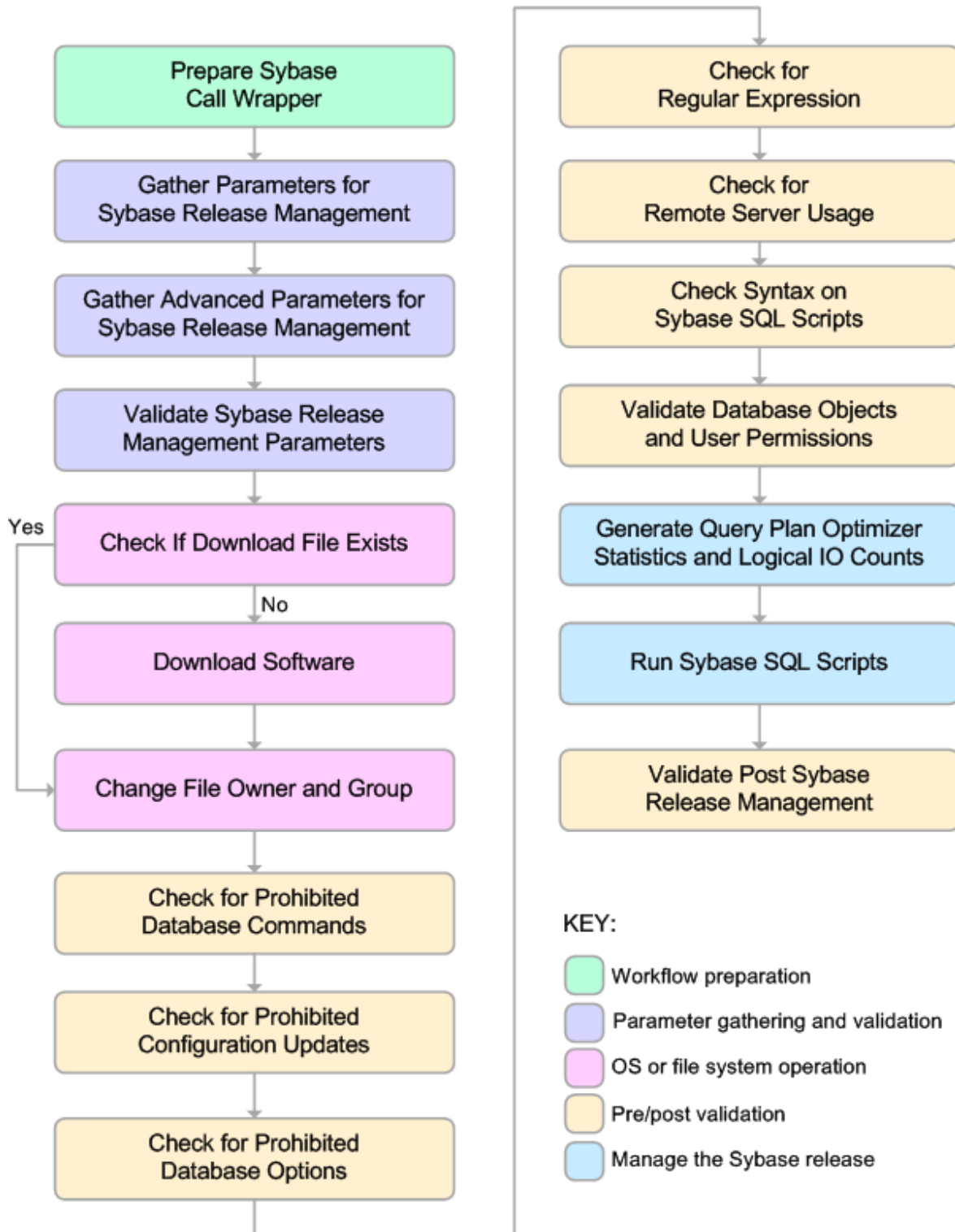
This workflow validates the SQL scripts in the following ways:

1. Checks whether the SQL statements contain any of the specified Prohibited Database Commands..
2. Checks whether the SQL statements contain any prohibited configuration updates defined in the `sysconfigures` system catalog—unless you specifically approve them in the Approved Configuration Updates parameter.
3. Checks whether the SQL statements contain any prohibited database options defined in the `spt_values` system catalog—unless you specifically approve them in the Approved Database Options parameter.
4. Checks whether the SQL statements match any of the specified prohibited Regular Expressions.
5. Checks whether the SQL statements contain the following remote server usage commands:
`create proxy_table`, `sp_addserver`, or `sp_dropserver`.
6. If you set the Run Check Syntax flag, checks whether the SQL statements have valid syntax.
7. Checks that the database objects used in the script exist and are available and that the user has permission to modify the database objects.

If any of the validations fail, the workflow will output the offending SQL line to `stdout`, return an error status, and the SQL scripts will not be executed.

Steps Executed

The "Sybase Release Management" workflow includes the following steps. Each step must complete successfully before the next step can start. If a step fails, the workflow reports a failure and all subsequent steps are skipped.



Steps Used in Sybase Release Management:

Workflow Step	Description
Prepare Sybase Call Wrapper	This step constructs the commands that will be used to execute subsequent workflow steps as either the OS administrative user or the owner of the Sybase ASE installation. The step also creates utility parameters that will be used by subsequent steps.
Gather Parameters For Sybase Release Management	This step accepts the basic input parameters for the " Sybase Release Management " workflow. The parameters will be used in subsequent steps.
Gather Advanced Parameters for Sybase Release Management	This step accepts the advanced input parameters for the " Sybase Release Management " workflow. The parameters will be used in subsequent steps.
Validate Sybase Release Management Parameters	This step validates the input parameters that manage the Sybase ASE release: the required input parameters have values, the SQL script files exist or will be downloaded, the Sybase ASE database is online, and the flag parameters have appropriate yes or no values.
Check if Download File Exists	This step determines whether one or more specified files already exist on the target server.
Download Software	This step downloads a list of files to a specified location on the target server.
Change File Owner and Group	This step changes the ownership and group of each file specified. A warning is issued for files that are not found.
Check for Prohibited Database Commands	This step checks the SQL scripts for any invalid database commands that you specify in the Prohibited Database Commands parameter.
Check for Prohibited Configuration Updates	This step checks the SQL scripts for any invalid <code>sp_configure</code> configuration updates. You can specify which configuration updates are valid with the Approved Configuration Updates parameter.
Check for Prohibited Database Options	This step checks the SQL scripts for any invalid <code>sp_dboption</code> database options. You can specify which database options are valid with the Approved Database Options parameter.
Check for Regular Expressions	This step checks the SQL scripts for any text that matches what you specify in the Regular Expressions parameter. This step is skipped if no Regular Expressions are specified.
Check for Remote Server Usage	This step checks the SQL scripts for the usage of remote servers. The keywords <code>create proxy_table</code> , <code>sp_addserver</code> , and <code>sp_dropserver</code> indicate that a remote server is used.

Steps Used in Sybase Release Management:, continued

Workflow Step	Description
Check Syntax on Sybase SQL Scripts	If the Run Check Syntax flag is set, this step checks the SQL scripts for any syntax errors. The underlying code will not be executed.
Validate Database Objects and User Permissions	This step checks the SQL scripts to ensure that: <ul style="list-style-type: none"> • Database objects used in the script exist and are available. • The user has permission to modify the database objects.
Generate Query Plan Optimizer Statistics and Logical IO Counts	This step runs the <code>isql</code> (Interactive SQL parser to Adaptive Server) utility to simulate the execution of the SQL script files—without running the actual T-SQL code. If the following input flags are set: <ul style="list-style-type: none"> • Generate Query Plan—the step will show a query plan. • Generate Optimizer Statistics—the step will show the statistics time. • Generate Logical I/O Counts—the step will show the statistics of logical/physical input and output.
Run Sybase SQL Scripts	This step runs the <code>isql</code> (Interactive SQL parser to Adaptive Server) utility to deploy and execute the SQL script files against the target Sybase ASE databases—only if the run flag is set, no errors were found in the SQL scripts, and the Generate Query Plan, Generate Optimizer Statistics, and Generate Logical I/O Counts flags are all set to N.
Validate Post Sybase Release Management	This step sends messages to steplog that the workflow was successful: <ul style="list-style-type: none"> • Input TSQL/config/dboptions files have been verified successfully and have not been run. • All Sybase Release Management scripts ran successfully.

Note: For input parameter descriptions and defaults, see ["Parameters for Sybase Release Management" on page 795](#).

How to Run this Workflow

The following instructions show you how to customize and run the ["Sybase Release Management"](#) workflow in your environment.

The workflow provides default values for some parameters. These default values are usually sufficient for a "typical" installation. You can override the defaults by specifying parameter values in the deployment. You can also expose additional parameters in the workflow, if necessary, to accomplish more advanced scenarios. Any parameters not explicitly specified in the deployment will have the default values listed in ["Parameters for Sybase Release Management"](#) on page 795.

Note: Before following this procedure, review the ["Prerequisites for this Workflow"](#) on page 781, and ensure that all requirements are satisfied.

To use the Sybase Release Management workflow:

1. Create a deployable copy of the workflow.
2. Determine the values that you will specify for the following parameters:

Input Parameters for Prepare Sybase Call Wrapper

Parameter Name	Default Value	Required	Description
Call Wrapper	See description	optional	Command that will execute this step (or subsequent steps) as a specific user. For UNIX targets, the default is: <code>/opt/hp/dma/client/jython.sh</code> running as root For Windows targets, the default is: <code>jython</code> running as Administrator
Sybase OS User Name	sybase	required	OS user who owns the Sybase ASE installation directory.

Input Parameters for Gather Parameters For Sybase Release Management

Parameter Name	Default Value	Required	Description
SQL Scripts	no default	required	Comma-separated list of SQL script files that will be released to (executed on) the target Sybase ASE database. These files can contain various SQL queries, configuration parameters, and database options. For example: <code>mysql.sql</code> Note: List the SQL script files in the order in which they need to be executed.

Input Parameters for Gather Advanced Parameters For Sybase Release Management

Parameter Name	Default Value	Required	Description
Approved Configuration Updates		optional	Comma-separated list of configuration updates (<code>sp_configure</code> commands) that are allowed to be performed by the specified SQL Scripts. This overrides configuration updates that would normally be prohibited. For example: <code>systemwide password expiration</code>
Approved Database Options		optional	Comma-separated list of database options (<code>sp_dboption</code> commands) that are allowed to be configured by the specified SQL Scripts. This overrides database options that would normally be prohibited. For example: <code>select into/bulkcopy/pllsort</code>
Generate Logical I/O Counts	N	optional	Set to Y to enable generation of logical/physical input or output counts required to execute each query in the specified SQL Scripts.
Generate Optimizer Statistics	N	optional	Set to Y to enable generation of Optimizer Statistics for each query in the specified SQL Scripts.
Generate Query Plan	N	optional	Set to Y to enable the generation of the Optimizer Query Plan required to execute each query in the specified SQL Scripts.
Prohibited Database Commands		optional	Comma-separated list of database commands (<code>sp_dboption</code> commands) that will be ignored in the specified SQL Scripts. For example: <code>dbo use only,select into/bulkcopy/pllsort</code>
Regular Expressions		optional	Comma-separated list of formatted regular expressions that will be searched for in the specified SQL Scripts. The expression can fall anywhere in the SQL command line. For example: <code>drop table, truncate table</code>

Note: This is the minimum set of parameters required to run this workflow. You may need to expose additional parameters depending on your objectives.

See "[Parameters for Sybase Release Management](#)" on page 795 for detailed descriptions of all input parameters for this workflow, including default values.

3. In the workflow editor, expose any additional parameters that you need.

4. Save the changes to the workflow (click Save in the lower right corner).
5. Create a new deployment.
6. On the Parameters tab, specify values for the required parameters listed in step 2 and any additional parameters that you have exposed. You do not need to specify values for those parameters whose default values are appropriate for your environment.
7. On the Targets tab, specify one or more targets for this deployment.
8. Save the deployment (click Save in the lower right corner).
9. Run the workflow using this deployment.

To verify the results:

The workflow will complete and report SUCCESS on the Console if it has run successfully. If an error occurs during workflow execution, the error is logged, and the workflow terminates in the FAILURE state.

Optional: If you want to further verify the results:

Log in to your database to make sure that whatever you created or modified was actually done.

To view the output:

The workflow generates an output file for each SQL script file that is executed and stores it in the `/tmp` directory. Open the output files to see the execution results for the T-SQL, Adaptive Server configuration changes, and database option settings. The workflow also writes the execution output for SQL script execution in the DMA Steplog.

If you have chosen to view the optimizer query plan or to generate the statistics before the query execution, these files will also be created and stored in the `/tmp` directory.

Sample Scenarios

This topic shows you typical parameter values for different use cases for the "Sybase Release Management" workflow.

Scenario 1: Check the SQL script files for prohibited configuration updates, prohibited database options, and invalid syntax; then deploy and execute the SQL scripts

In this scenario, you only specify the SQL Scripts parameter since this scenario takes advantage of many parameter defaults. Running this scenario will check the SQL script files for:

- The normal prohibited configuration updates (`sp_configure` commands).
- The normal prohibited database options (`sp_dboption` commands).
- Any invalid syntax of the SQL queries.
- No database commands—since no prohibited database commands are specified by default.
- No regular expressions—since no regular expressions are specified by default.

It will not simulate executing the SQL scripts to generate a query plan, optimizer statistics, or logical/physical input and output counts. If all the tests pass, the SQL scripts are deployed and executed against the target Sybase ASE databases.

Input Parameters for Gather Parameters For Sybase Release Management

Parameter Name	Example Value	Description
SQL Scripts	mysql.sql	Comma-separated list of SQL script files that will be released to (executed on) the target Sybase ASE database. These files can contain various SQL queries, configuration parameters, and database options. For example: mysql.sql Note: List the SQL script files in the order in which they need to be executed.

Be sure that the default values for all remaining input parameters are appropriate for your environment (see "Parameters for Sybase Release Management" on page 795).

Scenario 2: Check the SQL script files for specified prohibited database commands, prohibited configuration updates, prohibited database options, prohibited regular expressions, and invalid syntax; simulate running the SQL scripts to generate statistics; then deploy and execute the SQL scripts

In this scenario, you take advantage of the customized checks and reports that are available in Sybase Release Management. Running this scenario will check the SQL script files for:

- Prohibited database commands (`sp_dboption` commands) that you specify.
- Prohibited configuration updates (`sp_configure` commands) except for the updates that you specifically approve.
- Prohibited database options (`sp_dboption` commands) except for the options that you specifically approve.
- Prohibited regular expressions that you specify.
- Any invalid syntax of the SQL queries.

Then this scenario will simulate running the SQL scripts—without actually executing them—to give the following

- Show the query plan.
- Estimate the time required to execute the SQL scripts.
- Show the logical and physical input and output counts that will be required to execute each query.

If all the tests pass, the SQL scripts are deployed and executed against the target Sybase ASE databases.

Input Parameters for Gather Parameters For Sybase Release Management

Parameter Name	Example Value	Description
SQL Scripts	<code>mysql.sql</code>	Comma-separated list of SQL script files that will be released to (executed on) the target Sybase ASE database. These files can contain various SQL queries, configuration parameters, and database options. For example: <code>mysql.sql</code> Note: List the SQL script files in the order in which they need to be executed.

Input Parameters for Gather Advanced Parameters For Sybase Release Management

Parameter Name	Example Value	Description
Approved Configuration	see description	Comma-separated list of configuration updates (<code>sp_configure</code> commands) that are allowed to be performed by the specified SQL

Input Parameters for Gather Advanced Parameters For Sybase Release Management, continued

Parameter Name	Example Value	Description
Updates		Scripts. This overrides configuration updates that would normally be prohibited. For example: <code>systemwide password expiration</code>
Approved Database Options	see description	Comma-separated list of database options (<code>sp_dboption</code> commands) that are allowed to be configured by the specified SQL Scripts. This overrides database options that would normally be prohibited. For example: <code>select into/bulkcopy/pllsort</code>
Generate Logical I/O Counts	Y	Set to Y to enable generation of logical/physical input or output counts required to execute each query in the specified SQL Scripts.
Generate Optimizer Statistics	Y	Set to Y to enable generation of Optimizer Statistics for each query in the specified SQL Scripts.
Generate Query Plan	Y	Set to Y to enable the generation of the Optimizer Query Plan required to execute each query in the specified SQL Scripts.
Prohibited Database Commands	see description	Comma-separated list of database commands (<code>sp_dboption</code> commands) that will be ignored in the specified SQL Scripts. For example: <code>dbo use only,select into/bulkcopy/pllsort</code>
Regular Expressions	see description	Comma-separated list of formatted regular expressions that will be searched for in the specified SQL Scripts. The expression can fall anywhere in the SQL command line. For example: <code>drop table, truncate table</code>

Be sure that the default values for all remaining input parameters are appropriate for your environment (see ["Parameters for Sybase Release Management" on the next page](#)).

Parameters for Sybase Release Management

The following tables describe the required and optional input parameters for this workflow. Some of these parameters may not be initially visible in a deployment. For some parameters, if you do not specify a value for a parameter, a default value is assigned.

Only those parameters that are configurable in a standard deployment are listed here. Input parameters that must be mapped to output parameters of previous steps are not listed.

Parameters Defined in this Step: Prepare Sybase Call Wrapper

Parameter Name	Default Value	Required	Description
Call Wrapper	See description	optional	Command that will execute this step (or subsequent steps) as a specific user. For UNIX targets, the default is: <code>/opt/hp/dma/client/jython.sh</code> running as root For Windows targets, the default is: <code>jython</code> running as Administrator
Sybase OS User Name	sybase	required	OS user who owns the Sybase ASE installation directory.

Parameters Defined in this Step: Gather Parameters For Sybase Release Management

Parameter Name	Default Value	Required	Description
SQL Scripts	no default	required	Comma-separated list of SQL script files that will be released to (executed on) the target Sybase ASE database. These files can contain various SQL queries, configuration parameters, and database options. For example: <code>mysql.sql</code> Note: List the SQL script files in the order in which they need to be executed.
Sybase Home	see description	required	Sybase ASE installation directory (absolute path). For example: <code>/opt/sybase/ase_1503</code> If the Discovery workflow has previously been executed, this parameter value is automatically detected. You can specify a different installation directory if you prefer. The default is the metadata value for <code>Instance.sybase home</code> .
Sybase Password	see description	required	Adaptive Server (instance) login password for the Sybase User. If the Discovery workflow has previously been executed, this parameter value is automatically detected. You can specify a different password if you prefer. The default is the metadata value for <code>Instance.password</code> .

Parameters Defined in this Step: Gather Parameters For Sybase Release Management, continued

Parameter Name	Default Value	Required	Description
Sybase User	see description	required	<p>Adaptive Server (instance) user who will execute the specified SQL Scripts on the target. For example: admin</p> <p>If the Discovery workflow has previously been executed, this parameter value is automatically detected. You can specify a different Sybase ASE user if you prefer.</p> <p>The default is the metadata value for <code>Instance.user</code>.</p>

Parameters Defined in this Step: Gather Advanced Parameters For Sybase Release Management

Parameter Name	Default Value	Required	Description
Approved Configuration Updates		optional	<p>Comma-separated list of configuration updates (<code>sp_configure</code> commands) that are allowed to be performed by the specified SQL Scripts. This overrides configuration updates that would normally be prohibited.</p> <p>For example: <code>systemwide password expiration</code></p>
Approved Database Options		optional	<p>Comma-separated list of database options (<code>sp_dboption</code> commands) that are allowed to be configured by the specified SQL Scripts. This overrides database options that would normally be prohibited.</p> <p>For example: <code>select into/bulkcopy/pllsort</code></p>
Download Location	/tmp	optional	Location where the SQL Scripts files will be downloaded from software repository if they are not found on the target server.
Generate Logical I/O Counts	N	optional	Set to Y to enable generation of logical/physical input or output counts required to execute each query in the specified SQL Scripts.
Generate Optimizer Statistics	N	optional	Set to Y to enable generation of Optimizer Statistics for each query in the specified SQL Scripts.
Generate Query Plan	N	optional	Set to Y to enable the generation of the Optimizer Query Plan required to execute each query in the specified SQL Scripts.
Prohibited Database Commands		optional	<p>Comma-separated list of database commands (<code>sp_dboption</code> commands) that will be ignored in the specified SQL Scripts.</p> <p>For example: <code>dbo use only,select into/bulkcopy/pllsort</code></p>
Regular Expressions		optional	<p>Comma-separated list of formatted regular expressions that will be searched for in the specified SQL Scripts. The expression can fall anywhere in the SQL command line.</p> <p>For example: <code>drop table, truncate table</code></p>

Parameters Defined in this Step: Gather Advanced Parameters For Sybase Release Management, continued

Parameter Name	Default Value	Required	Description
Run Check Syntax	Y	optional	Set to Y to enable syntax checking of the queries included in the specified SQL Scripts .
Run SQL Scripts Flag	Y	optional	Set to Y to perform the checks and run the specified SQL Scripts on the target. Set to N to only perform the checks.

Sybase - Patch to Home and Instance

This workflow applies an Emergency Bug Fix (EBF) patch to an existing Sybase Adaptive Server Enterprise (ASE) version 15.7 installation. It uses a binary setup.bin installation utility to apply the patch and then runs post-patching scripts.

If you have problems after applying the patch, you can remove it by running ["Sybase - Rollback from Home and Instance" on page 822](#).

To use this workflow in your environment, see the following information:

Topic	Information Included
"Prerequisites for this Workflow"	List of prerequisites that must be satisfied before you can run this workflow
"How this Workflow Works"	Information about what the workflow does, including validation checks performed, steps executed, and a high-level process flow
"How to Run this Workflow"	Instructions for running this workflow in your environment
"Sample Scenario"	Examples of typical parameter values for this workflow
"Parameters for Sybase - Patch Home and Instance" on page 814	List of input parameters for this workflow

Note: The documentation for this workflow contains steps that are referred to by their base names. The names in the DMA user interface may have a version appended, for example, v2.

Prerequisites for this Workflow

Be sure that the following prerequisites are satisfied before you run the ["Sybase - Patch to Home and Instance" on the previous page](#) workflow:

- The latest DMA solution packs require the latest DMA platform. To use the latest solution packs, update the DMA platform. DMA 10.40 solution packs are supported on DMA 10.40 (and later).
- You have installed the DMA Database Patching solution pack.
- You need to have Sybase provisioned and operational. You can do this by running the following workflows in the DMA Database Provisioning Solution Pack:
 - Sybase Provision Software
 - Sybase Provision Instance v2
- You have read access to all specified inventory pointers (Linux/UNIX).
- You have a Sybase support contract and have downloaded the appropriate patches either to the software repository or to the target machine.
- You have unchallenged sudo access to a user (typically root) who can access all required files and directories to download and execute.

For more information about prerequisites for Sybase, refer to the [Sybase Product Documentation](#).

How this Workflow Works

The following information describes how the Sybase - Patch to Home and Instance workflow works:

Overview

This workflow does the following things in the order shown:

- The initial steps of the workflow prepare it to patch the Sybase Home. The workflow processes and validates user input parameters, executes commands used in subsequent steps, downloads any required files, takes backup of the database, database tables, and server configuration, and shuts down the Sybase server. Default values are set for optional parameters if no values are specified.
- The workflow applies the patch to the Sybase Database Home.
- The workflow applies the patch to the Sybase Instances.
- The final steps of the workflow allow the workflow to end cleanly. The workflow restarts Sybase server, brings Sybase database online, and discovers Sybase database. Then it cleans up the downloaded files.

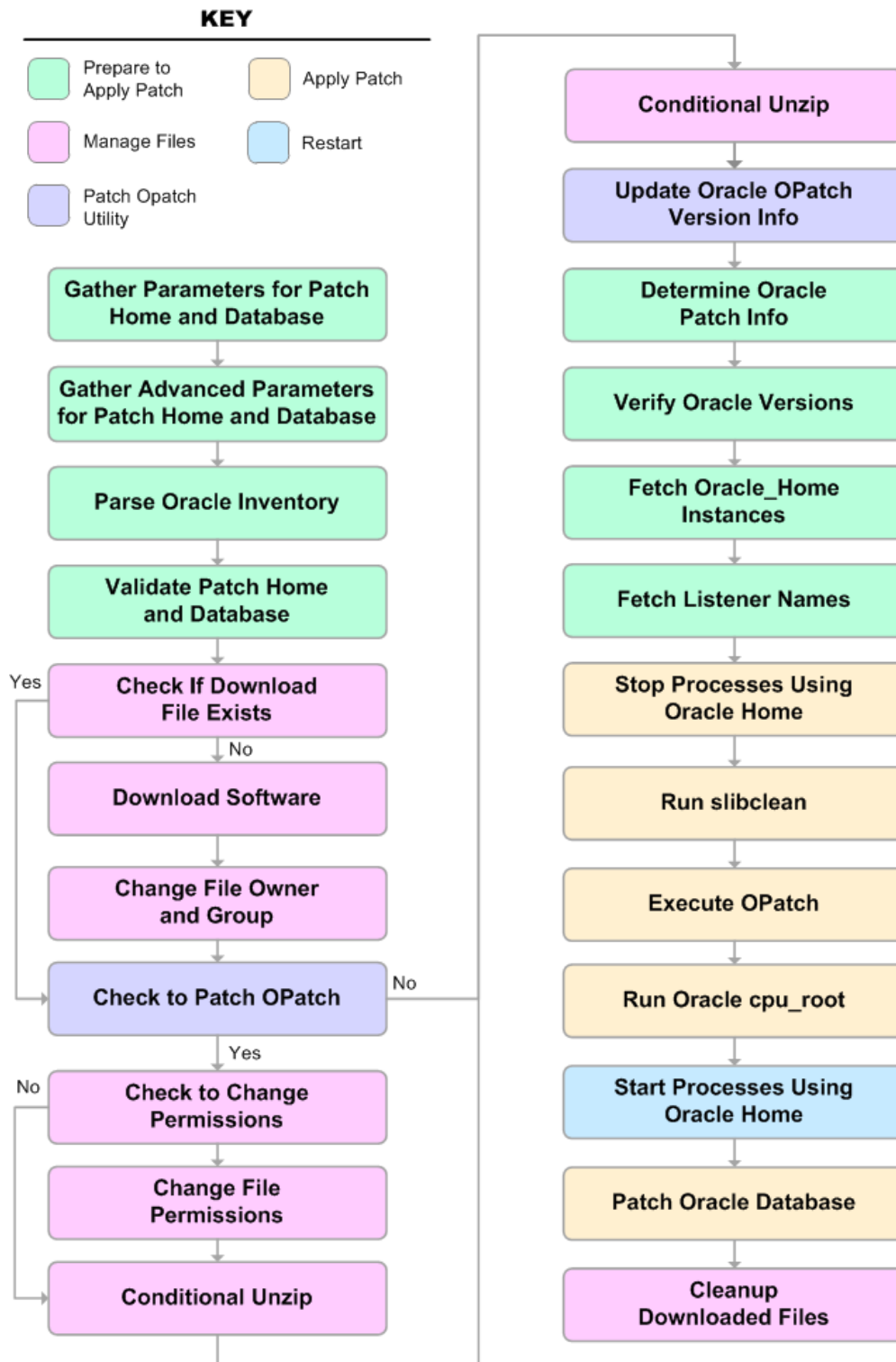
Validation Checks Performed

Much of the validation centers on the input parameters:

- The input parameters have the proper syntax (no special characters or spaces).
- Files exist or have valid specifications if they do not exist.
- The supplied patch update applies to the current Sybase Database version.

Steps Executed

The Sybase - Patch to Home and Instance workflow includes the following steps. Each step must complete successfully before the next step can start. If a step fails, the workflow reports a failure and all subsequent steps are skipped.



Steps Used in Sybase - Patch to Home and Instance

Workflow Step	Description
Gather Parameters for Sybase Patch Home and Instance	This step gathers the required parameters for the Sybase - Patch to Home and Instance workflow.
Gather Advanced Parameters for Sybase Patch Home and Instance	This step gathers the optional advanced parameters for the Sybase - Patch to Home and Instance workflow.
Prepare Sybase Call Wrapper v2	This step constructs the commands that will be used to execute subsequent workflow steps as either the OS administrative user or the owner of the Sybase ASE installation.
Validate Parameters for Sybase Patch Home and Instance	This step validates the values specified for the input parameters used by the Sybase - Patch to Home and Instance workflow. It also sets the values of various output parameters that will be consumed by subsequent steps.
Download Software	This step downloads a list of files to a specified location on the target server.
Uncompress Sybase File v2	For each supplied file, this step extracts the contents of the archive file (or files).
Run Sybase DBCC Checks v2	This step runs the specified database consistency checker (DBCC) checks to ensure that no database tables or objects have become corrupted. The output of these checks is printed in the step log and stored in files under the specified directory. .
Backup Sybase System Databases v2	This step takes backup the user databases, schemas, and transaction logs and stores them in the backup directory.
Backup Sybase System Tables v2	This step takes backup the system tables and store the backup in the backup directory.
Backup Sybase Server Configuration v2	This step takes backup the database server level configuration details and stores them in the backup directory.
Backup Sybase Directory v2	This step creates a backup copy of the entire Sybase installation folder and Sybase device files.
Validate Patch for Target Platform Compatibility	This step validates the following: <ul style="list-style-type: none"> • If the patch and the target OS and architecture (64-bit or 32-bit) are compatible • If the intended patch is more recent than the existing patch on the Sybase installation

Steps Used in Sybase - Patch to Home and Instance, continued

Workflow Step	Description
	<ul style="list-style-type: none"> • If the ESD number of the patch is greater than the ESD number of the current sybase installation • If the EBF number of the patch is greater than the EBF number of the current sybase installation
Shutdown Sybase Servers v2	This step shuts down the Sybase server prior to installing the EBF patch.
Install Sybase Patch	This step installs EBF patch for Sybase ASE.
Cleanup Downloaded Files v2	This step removes files and archives that were downloaded to the target system during previous workflow steps.
Startup Sybase Servers v2	This step invokes the Sybase commands to startup the Sybase servers. It can startup dataserver, backupserver, and monserver if proper input parameter values are provided. It verifies that the servers have been started successfully by checking the process running on the operating system.
Copy Directory	This step creates a backup copy of the entire Sybase installation folder and Sybase device files.
Run Sybase Post Patch System Scripts	This step executes the Sybase system scripts necessary as configured in the workflow deployment post EBF patch for the Sybase installation on the target server.
Bring Sybase Database Online v2	This step brings the user-defined databases online within the database server.
Shutdown Sybase Servers	This step shuts down the dataserver instance.
Startup Sybase Servers v2	This step implements the Sybase commands to startup the Sybase servers. It can startup dataserver, backupserver, and monserver if proper input parameter values are provided. It verifies that the servers have been started successfully by checking the process running on the operating system.
Disable Sybase Database Object DDL Text v2	This step disables access to the database object's DDL text.
Cleanup Downloaded Files v2	This step removes files and archives that were downloaded to the target system during previous workflow steps.
Run Sybase DBCC Checks v2	This step runs the specified database consistency checker (DBCC) checks to ensure that no database tables or objects have become corrupted. The output of these checks is printed in the step log and stored in files under the specified directory.
Update Sybase Version v2	This step updates the Sybase Instance.Version metadata information for a Sybase Dataserver Instance.

Steps Used in Sybase - Patch to Home and Instance, continued

Workflow Step	Description
Discover Sybase Databases v2	This step audits the server's physical environment looking for Sybase databases and instances.

For parameter descriptions and defaults, see ["Parameters for Sybase - Patch Home and Instance"](#).

How to Run this Workflow

The following instructions show you how to customize and run the ["Sybase - Patch to Home and Instance"](#) workflow in your environment.

The workflow provides default values for some parameters. These default values are usually sufficient for a "typical" installation. You can override the defaults by specifying parameter values in the deployment. You can also expose additional parameters in the workflow, if necessary, to accomplish more advanced scenarios. Any parameters not explicitly specified in the deployment will have the default values listed in ["Parameters for Sybase - Patch Home and Instance"](#) on page 814.

Note: Before following this procedure, review the ["Prerequisites for this Workflow"](#) on page 799, and ensure that all requirements are satisfied.

To run this workflow, you need to set your parameters differently depending on the location and status of your EBF patch. Use the following table to choose the method that matches your situation.

To use the Sybase - Patch to Home and Instance workflow:

1. Create a deployable copy of the workflow.
2. Determine the values that you will specify for the following parameters:

Basic Parameters

Parameter Name	Default Value	Required	Description
Call Wrapper	see description	required	Command that will execute this step (or subsequent steps) as a specific user. For UNIX targets, the default is: <code>/opt/hp/dma/client/jython.sh</code> running as root
Sybase OS User Account	sybase	required	OS user who owns the Sybase ASE installation directory. This is the directory specified in the Sybase Install Directory parameter, where the Sybase ASE binaries will be installed.
Sybase Installation Location	no default	required	The directory where the patch will be installed. This is equivalent to the \$SYBASE environment variable. For example: <code>/home/sybase/ASE_15_5</code> .
Sybase Admin Password	no default	required	The password for the ASE system administrator (specified in the Sybase Admin Login parameter). This password is assigned after ASE is provisioned to validate the installation.
Sybase Admin Login	no default	required	The Sybase ASE user who is the ASE system administrator and possesses all ASE privileges.
Sybase Patch Archive	no default	required	The name of sybase binary EBF patch file. For example: <code>EBF18380.tgz</code> .
Web Service Password	no default	required	DMA Web Service password of DMA user.
Web Service URL	no default	required	The path for DMA web service.
Web Service User	no default	required	The DMA user.
Backup Server Name	no default	required	The Backup Server name associated with the Adaptive Server (dataserver). Backup Server is responsible for performing backups (dumps) and restores (loads) on selected databases and transaction logs. If not specified, it will not be rebooted after rolling back the patch. For example: <code>BS_DEV_300</code> .

Advanced Parameters

Parameter Name	Default Value	Required	Description
Backup Sybase Server Configuration v2	yes	optional	<p>Flag that determines whether to backup Sybase system configuration before EBF patch is applied.</p> <p>If yes, Sybase system configuration backup is taken before EBF patching. If no, Sybase system configuration backup is not taken.</p> <p>Valid values are y, yes, true, n, no, or false. Default is yes.</p>
Backup Sybase System Databases v2	yes	optional	<p>Flag that determines whether to backup Sybase system database before EBF patch is applied.</p> <p>If yes, Sybase system database backup is taken before EBF patching. If no, Sybase system database backup is not taken.</p> <p>Valid values are y, yes, true, n, no, or false. Default is yes.</p>
Backup Sybase System Tables v2	yes	optional	<p>Flag that determines whether to backup Sybase system tables before EBF patch is applied.</p> <p>If yes, Sybase system tables backup is taken before EBF patching. If no, Sybase system tables backup is not taken.</p> <p>Valid values are y, yes, true, n, no, or false. Default is yes.</p>
Clean on Failure	true	optional	<p>Flag that determines whether to clean up on workflow failure. If true, downloaded files will be cleaned up on failure of workflow.</p> <p>Valid values are y, yes, true, n, no, or false. Default is yes.</p>
Clean on Success	true	optional	<p>Flag that determines whether to clean up on workflow success. If true, downloaded files will be cleaned up on success of workflow.</p> <p>Valid values are y, yes, true, n, no, or false. Default is yes.</p>
DBCC Check List	checkdb, checkalloc,	optional	<p>The comma-separated list of database consistency checker (DBCC) checks that you want to</p>

Advanced Parameters, continued

Parameter Name	Default Value	Required	Description
	checkcatalog		run to check whether there are issues with the database before and after applying the patch. Default value is checkdb, checkalloc, or checkcatalog.
DBCC Errorlog Location	/SYBASE_OS_HOME_DIR/dbcclog	optional	The fully-qualified directory path where you want to store the DBCC run log results (output files) for pre-patch and post-patch checks. The default value is /SYBASE_OS_HOME_DIR/dbcclog.
Run Sybase DBCC Check v2	yes	optional	Flag that determines whether to run Sybase DBCC patch before EBF patch is applied. If yes, Sybase DBCC check will be done before EBF patching. If no, DBCC check will be skipped. Valid values are y, yes, true, n, no, or false. Default is yes.
Sybase Admin Login:		required	Required: The Admin Login for the Sybase ASE system administrator. It is used to validate the installation by logging in to the server
Sybase Admin Password	no default	required	The password for the Sybase ASE system administrator. It is used to validate the installation by logging in to the server.
Sybase Archive Location	/tmp/dma/archive	optional	Fully qualified directory on the target server where the Sybase ASE installation binaries will be downloaded, or the location where the ASE software installation .tar or .tgz file is located. The default is /tmp/dma/archive.
Sybase Backup Location	/<SYBASE_OS_HOME_DIR>/syb_backup	optional	The absolute directory path where the backup of the Sybase ASE installation will be stored before applying the patch. Default is /<SYBASE_OS_HOME_DIR>/syb_backup.
Sybase Backupserver Name	no default	optional	The Backup Server name associated with the Adaptive server (dataserver). Backup Server is responsible for performing backups (dumps) and restores (loads) on

Advanced Parameters, continued

Parameter Name	Default Value	Required	Description
			selected databases and transaction logs. If not specified, it will not be rebooted after applying the patch.
Sybase Dataserver Name	See description	optional	<p>The Adaptive Server instance running on the target machine with the dataserver process. The Adaptive server component manages databases and users, records the location of data on disks, maps logical data descriptions to physical data storage, and manages data and procedure caches in memory.</p> <p>The default value is set from the deployment instance.</p>
Sybase Installation Location	no default	required	The directory where the Sybase Software was provisioned.
Sybase Master Device Name	master	optional	<p>Name of the Sybase system device where the master database is mounted and running. If the default device for the master database is not master.dat this is required. If using raw device provisioning and the master database is mounted on dev/raw/raw1, then the value can be raw1.</p> <p>The default is master.</p>
Sybase Monitorserver Name	no default	optional	The Monitor Server name associated with the Adaptive server (dataserver). The Monitor Server is responsible for monitoring and supervising the Adaptive Server. If not specified, it will not be rebooted after applying the patch to reflect the EBF updates
Sybase OS User Account	sybase	required	Sybase account OS user who owns the Sybase ASE installation directory and instance. The default is sybase.
Sybase Patch Archive	no default	required	<p>The name of sybase binary EBF patch file.</p> <p>For example: EBF18380.tgz.</p>
Sybase Postpatch System Script List	installmaster, instmsgs.ebf, installcommit	optional	Comma-separated list of Sybase provided scripts to be run after patching the Sybase instance. These scripts make the appropriate

Advanced Parameters, continued

Parameter Name	Default Value	Required	Description
			changes to the system tables and procedures and update the Adaptive Server version. The default is 'installmaster, instmsgs.ebf, or installcommit.
Sybase Servers Errorlog File Format	See description	optional	Adaptive Server errorlog file format. Used to allow a non-standard SAP server errorlog file name. Specify your own format that includes '%s'. The '%s' will be replaced with the Adaptive Server name. For example, if the format is set to 'errorLog_%s' and the server name is 'NY_DS', the workflow will create the errorlog file 'errorLog_NY_DS'. This also applies if any backupserver or monserver are being patched and rebooted. The default is '%s.log'.
Sybase Staging Location	/tmp/dma/staging	optional	The staging location on the target server where the Sybase ASE binaries will be stored prior to installation. The default is /tmp/dma/staging.
Sybase System Scripts Location	\$SYBASE/ASE-15_0/scripts	optional	Fully qualified directory path where Post Install Script List (the Sybase provided scripts) is available to run after applying the EBF patch. These scripts make the appropriate changes to the system tables and procedures and update the ASE version. The default is \$SYBASE/ASE-15_0/scripts.
Sybase Version	See description	optional	Sybase Version that is installed on the target machine to be patched with provided EBF. Valid values are 15.0.3 or 15.5. Default: It will be extracted from the target machine Sybase installation.
User Defined Patch Responsefile	no default	optional	The silent install response file name. If not provided, then the workflow will use the deployment parameters to create a response file that will be used for patching Sybase. If the response file is provided, the workflow will override

Advanced Parameters, continued

Parameter Name	Default Value	Required	Description
			the response file parameters with values from the silent response file. If the response file is invalid or has a problem, the workflow behavior may be unpredictable.

3. In the workflow editor, expose any additional parameters that you need. You will specify values for those parameters when you create the deployment.
4. Save the changes to the workflow (click **Save** in the lower right corner).
5. Create a new deployment.
6. On the Parameters tab, specify values for the required parameters listed in step 2. You do not need to specify values for those parameters whose default values are appropriate for your environment.
7. On the Targets tab, specify one or more targets for this deployment.
8. Save the deployment (click **Save** in the lower right corner).
9. Run the workflow using this deployment.

Note: See ["Parameters for Sybase - Patch Home and Instance" on page 814](#) for detailed descriptions of all input parameters for this workflow, including default values.

To verify the results:

The workflow will complete and report SUCCESS on the Console if it has run successfully. If an error occurs during workflow execution, the error is logged, and the workflow terminates in the FAILURE state.

See the Console page output for error messages that indicate whether problems occurred during the application of the patches.

Optional: If you want to further verify that the patch was successfully applied to the Sybase Database Instances associated with the Sybase Home:

1. Verify the EBF version by querying the global variable (@@version) value. It should match the EBF Patch Number specified.
2. Verify that all databases are online and users are able to log-in.
3. Run basic database consistency check commands, and ensure that no errors are reported.

Sample Scenario

This topic shows you typical parameter values for different use cases for the "[Sybase - Patch to Home and Instance](#)" workflow. The workflow applies Emergency Bug Fix (EBF) patch to an existing Sybase Adaptive Server Enterprise (ASE) version 15.7 installation. It uses a binary setup.bin installation utility to apply the patch and then runs post-patching scripts.

Input Parameters for Gather Parameters for Sybase Patch Home and Instance

Parameter Name	Example Value	Description
Call Wrapper	jython	Command that will execute this step (or subsequent steps) as a specific user.
Sybase OS User Account	sybase	OS user who owns the Sybase ASE installation directory. This is the directory specified in the Sybase Install Directory parameter, where the Sybase ASE binaries will be installed.
Sybase Installation Location	/opt/app/sybase	The directory where the patch will be installed. This is equivalent to the \$SYBASE environment variable.
Sybase Admin Login	sa	The Sybase ASE user who is the ASE system administrator and possesses all ASE privileges.
Sybase Patch Archive	EBF20953.tar	The name of Sybase binary EBF patch file.

Input Parameters for Gather Advanced Parameters for Sybase Patch Home and Instance

Parameter Name	Example Value	Description
Sybase Backupserver Name	BS_200	The Backup Server name associated with the Adaptive server (dataserver).
Sybase Master Device Name	raw1	Name of the Sybase system device where the master database is mounted and running.
Sybase Version	15.7	Sybase Version that is installed on the target machine to be patched with provided EBF.

Parameters for Sybase - Patch Home and Instance

The following tables describe the required and optional input parameters for this workflow.

Input Parameters Defined in this Step: Gather Parameters for Sybase Patch Home and Instance

Parameter Name	Default Value	Required	Description
Call Wrapper	see description	required	Command that will execute this step (or subsequent steps) as a specific user. For UNIX targets, the default is: <code>/opt/hp/dma/client/jython.sh</code> running as root
Sybase OS User Account	sybase	required	OS user who owns the Sybase ASE installation directory. This is the directory specified in the Sybase Install Directory parameter, where the Sybase ASE binaries will be installed.
Sybase Installation Location	no default	required	The directory where the patch will be installed. This is equivalent to the \$SYBASE environment variable. For example: <code>/home/sybase/ASE_15_5.</code>
Sybase Admin Password	no default	required	The password for the ASE system administrator (specified in the Sybase Admin Login parameter). This password is assigned after ASE is provisioned to validate the installation.
Sybase Admin Login	no default	required	The Sybase ASE user who is the ASE system administrator and possesses all ASE privileges.
Sybase Patch Archive	no default	required	The name of sybase binary EBF patch file. For example: <code>EBF18380.tgz.</code>
Web Service Password	no default	required	DMA Web Service password of DMA user.
Web Service URL	no default	required	The path for DMA web service (DMA URL).
Web Service User	no default	required	The DMA user.
Backup Server Name	no default	required	The Backup Server name associated with the Adaptive Server (dataserver). Backup Server is responsible for

Input Parameters Defined in this Step: Gather Parameters for Sybase Patch Home and Instance, continued

Parameter Name	Default Value	Required	Description
			<p>performing backups (dumps) and restores (loads) on selected databases and transaction logs. If not specified, it will not be rebooted after rolling back the patch.</p> <p>For example: BS_DEV_300.</p>

Additional Input Parameters Defined in this Step: Gather Advanced Parameters for Sybase Patch Home and Instance

Parameter Name	Default Value	Required	Description
Backup Sybase Server Configuration	yes	optional	<p>Flag that determines whether to backup Sybase system configuration before EBF patch is applied.</p> <p>If yes, Sybase system configuration backup is taken before EBF patching. If no, Sybase system configuration backup is not taken.</p> <p>Valid values are y, yes, true, n, no, or false. Default is yes.</p>
Backup Sybase System Databases	yes	optional	<p>Flag that determines whether to backup Sybase system database before EBF patch is applied.</p> <p>If yes, Sybase system database backup is taken before EBF patching. If no, Sybase system database backup is not taken.</p> <p>Valid values are y, yes, true, n, no, or</p>

Additional Input Parameters Defined in this Step: Gather Advanced Parameters for Sybase Patch Home and Instance, continued

Parameter Name	Default Value	Required	Description
			false. Default is yes.
Backup Sybase System Tables	yes	optional	<p>Flag that determines whether to backup Sybase system tables before EBF patch is applied.</p> <p>If yes, Sybase system tables backup is taken before EBF patching. If no, Sybase system tables backup is not taken.</p> <p>Valid values are y, yes, true, n, no, or false. Default is yes.</p>
Clean on Failure	true	optional	<p>Flag that determines whether to clean up on workflow failure. If true, downloaded files will be cleaned up on failure of workflow.</p> <p>Valid values are y, yes, true, n, no, or false. Default is yes.</p>
Clean on Success	true	optional	<p>Flag that determines whether to clean up on workflow success. If true, downloaded files will be cleaned up on success of workflow.</p> <p>Valid values are y, yes, true, n, no, or false. Default is yes.</p>
DBCC Check List	checkdb, checkalloc, checkcatalog	optional	The comma-separated list of database

Additional Input Parameters Defined in this Step: Gather Advanced Parameters for Sybase Patch Home and Instance, continued

Parameter Name	Default Value	Required	Description
			<p>consistency checker (DBCC) checks that you want to run to check whether there are issues with the database before and after applying the patch.</p> <p>Default value is checkdb, checkalloc, or checkcatalog.</p>
DBCC Errorlog Location	/SYBASE_OS_HOME_DIR/dbcclog	optional	<p>The fully-qualified directory path where you want to store the DBCC run log results (output files) for pre-patch and post-patch checks.</p> <p>The default value is /SYBASE_OS_HOME_DIR/dbcclog.</p>
Run Sybase DBCC Check	yes	optional	<p>Flag that determines whether to run Sybase DBCC patch before EBF patch is applied. If yes, Sybase DBCC check will be done before EBF patching. If no, DBCC check will be skipped.</p> <p>Valid values are y, yes, true, n, no, or false. Default is yes.</p>
Sybase Backup Location	/<SYBASE_OS_HOME_DIR>/syb_backup	optional	<p>The absolute directory path where the backup of the Sybase ASE installation will be stored before applying the patch.</p> <p>Default is /<SYBASE_OS_HOME_DIR>/syb_</p>

Additional Input Parameters Defined in this Step: Gather Advanced Parameters for Sybase Patch Home and Instance, continued

Parameter Name	Default Value	Required	Description
			backup.
Sybase Backupserver Name	no default	optional	The Backup Server name associated with the Adaptive server (dataserver). Backup Server is responsible for performing backups (dumps) and restores (loads) on selected databases and transaction logs. If not specified, it will not be rebooted after applying the patch.
Sybase Dataserver Name	See description	optional	<p>The Adaptive Server instance running on the target machine with the dataserver process. The Adaptive server component manages databases and users, records the location of data on disks, maps logical data descriptions to physical data storage, and manages data and procedure caches in memory.</p> <p>The default value is set from the deployment instance.</p>
Sybase Installation Location	no default	required	The directory where the Sybase Software was provisioned.
Sybase Master Device Name	master	optional	Name of the Sybase system device where the master database is mounted and running. If the

Additional Input Parameters Defined in this Step: Gather Advanced Parameters for Sybase Patch Home and Instance, continued

Parameter Name	Default Value	Required	Description
			<p>default device for the master database is not master.dat this is required. If using raw device provisioning and the master database is mounted on dev/raw/raw1, then the value can be raw1.</p> <p>The default is master.</p>
Sybase Monitorserver Name	no default	optional	<p>The Monitor Server name associated with the Adaptive server (dataserver). The Monitor Server is responsible for monitoring and supervising the Adaptive Server. If not specified, it will not be rebooted after applying the patch to reflect the EBF updates</p>
Sybase OS User Account	sybase	required	<p>Sybase account OS user who owns the Sybase ASE installation directory and instance. The default is sybase.</p>
Sybase Patch Archive	no default	required	<p>The name of sybase binary EBF patch file.</p> <p>For example: EBF18380.tgz.</p>
Sybase Postpatch System Script List	installmaster, instmsgs.ebf, installcommit	optional	<p>Comma-separated list of Sybase provided scripts to be run after patching the Sybase instance. These scripts make the appropriate</p>

Additional Input Parameters Defined in this Step: Gather Advanced Parameters for Sybase Patch Home and Instance, continued

Parameter Name	Default Value	Required	Description
			<p>changes to the system tables and procedures and update the Adaptive Server version.</p> <p>The default is 'installmaster, instmsgs.ebf, or installcommit.</p>
Sybase Servers Errorlog File Format	See description	optional	<p>Adaptive Server errorlog file format. Used to allow a non-standard SAP server errorlog file name. Specify your own format that includes '%s'. The '%s' will be replaced with the Adaptive Server name. For example, if the format is set to 'errorLog_%s' and the server name is 'NY_DS', the workflow will create the errorlog file 'errorLog_NY_DS'. This also applies if any backupserver or monserver are being patched and rebooted. The default is '%s.log'.</p>
Sybase Staging Location	/tmp/dma/staging	optional	<p>The staging location on the target server where the Sybase ASE binaries will be stored prior to installation.</p> <p>The default is /tmp/dma/staging.</p>
Sybase System Scripts Location	\$SYBASE/ASE-15_0/scripts	optional	Fully qualified directory path where Post Install

Additional Input Parameters Defined in this Step: Gather Advanced Parameters for Sybase Patch Home and Instance, continued

Parameter Name	Default Value	Required	Description
			<p>Script List (the Sybase provided scripts) is available to run after applying the EBF patch. These scripts make the appropriate changes to the system tables and procedures and update the ASE version.</p> <p>The default is \$SYBASE/ASE-15_0/scripts.</p>
Sybase Version	See description	optional	<p>Sybase Version that is installed on the target machine to be patched with provided EBF. Valid values are 15.0.3 or 15.5.</p> <p>Default: It will be extracted from the target machine Sybase installation.</p>
User Defined Patch Responsefile	no default	optional	<p>The silent install response file name. If not provided, then the workflow will use the deployment parameters to create a response file that will be used for patching Sybase. If the response file is provided, the workflow will override the response file parameters with values from the silent response file. If the response file is invalid or has a problem, the workflow behavior may be unpredictable.</p>

Sybase - Rollback from Home and Instance

Use this workflow if you encounter problems after applying a patch update. Only the last patch that was applied is rolled back.

This workflow requires previously created robust copy of ASE binary files which you may want to use to rollback the current Sybase ASE installation binaries.

To use this workflow in your environment, see the following information:

Topic	Information Included
"Prerequisites for this Workflow"	List of prerequisites that must be satisfied before you can run this workflow
"How this Workflow Works"	Information about what the workflow does, including validation checks performed, steps executed, and a high-level process flow
"How to Run this Workflow"	Instructions for running this workflow in your environment
"Sample Scenario"	Examples of typical parameter values for this workflow
"Parameters for Sybase - Rollback Patch from Home and Instance" on page 834	List of input parameters for this workflow

Prerequisites for this Workflow

Be sure that the following prerequisites are satisfied before you run the ["Sybase - Rollback from Home and Instance"](#) workflow:

- The latest DMA solution packs require the latest DMA platform. To use the latest solution packs, update the DMA platform. DMA 10.40 solution packs are supported on DMA 10.40 (and later).
- You have installed the DMA Database Patching Solution Pack.
- You need to have Sybase provisioned and operational. You can do this by running the following workflows in the DMA Database Provisioning Solution Pack:

Create Sybase Database

- You have read access to all specified inventory pointers (Linux/UNIX).
- You have unchallenged sudo access to a user (typically root) who can access all required files and directories to download and execute.
- For more information about prerequisites for Sybase database, refer to the [Sybase Product Documentation](#).

How this Workflow Works

The following information describes how the "Sybase - Rollback from Home and Instance" workflow works:

Overview

This workflow does the following things in the order shown:

- The Sybase - Rollback from Home and Instance workflow first makes the necessary preparations before actually rolling back the EBF patch. It processes and validates user input parameters. It makes sure files exist or have valid specifications. It executes commands used in subsequent steps. It takes backup of the database, database tables, and server configuration, and shuts down the Sybase server.
- Then the workflow rolls back the EBF patch to the Sybase Database Home.
- To finish up, the workflow restarts all the Sybase Instances and attempts to restart the Sybase database.

Validation Checks Performed

Much of the validation centers on the input parameters:

- The input parameters have the proper syntax (no special characters or spaces).
- Files exist or have valid specifications.

Steps Used in Sybase - Rollback from Home and Instance

Workflow Step	Description
Prepare Sybase Call Wrapper v2	This step constructs the commands that will be used to execute subsequent workflow steps as either the OS administrative user or the owner of the Sybase ASE installation.
Gather Parameters for Rollback Patch from Home and Instance	This step gathers the required parameters for the Sybase - Rollback from Home and Instance workflow.
Gather Advanced Parameters for Rollback EBF Patch from Home and Instance	This step gathers the optional advanced parameters for the Sybase - Rollback from Home and Instance workflow.
Validate Parameters for Rollback EBF Patch from Home and Instance	This step validates the values specified for the input parameters used by the Sybase - Rollback from Home and Instance workflow. It also sets the values of various output parameters that will be consumed by subsequent steps.
Backup Sybase System Tables v2	This step takes backup the system tables and store the backup in the backup directory.
Backup Sybase System Databases v2	This step takes backup the user databases, schemas, and transaction logs and stores them in the backup directory.
Backup Sybase Server Config	This step takes backup the database server level configuration details and stores them in the backup directory.
Backup Sybase Directory v2	This step copies the entire Sybase installation as well as Sybase device files.
Shutdown Sybase Servers v2	This step shuts down the Sybase server prior to rollback of the EBF patch.
Restore Adaptive Server Home	This step rolls back EBF patch applied for Sybase ASE and restores Sybase Home.
Copy Directory	This step takes backup of the Sybase installation folder.
Startup Sybase Servers v2	This step implements the Sybase commands to startup the Sybase servers. It can startup dataserver, backupserver, and monserver if proper input parameter values are provided. It verifies that the servers have been started successfully by checking the process running on the operating system.
Copy Directory	This step takes backup of the Sybase installation folder.
Verify Post Sybase Rollback Patch	This step performs post patch validation for Rollback of EBF/ESD for the current Sybase ASE installation.
Startup Sybase Servers v2	This step implements the Sybase commands to startup the Sybase servers. It can startup dataserver, backupserver, and monserver if proper input parameter values are provided. It verifies that the servers have been started successfully by checking the process running on the operating system.

Steps Used in Sybase - Rollback from Home and Instance, continued

Workflow Step	Description
Run Sybase Post Patch System Scripts	This step executes the Sybase system scripts necessary as configured in the workflow deployment post EBF patch rollback for the Sybase installation on the target server.
Shutdown Sybase Servers v2	This step shuts down the dataserver instance.
Shutdown Sybase Servers v2	This step shuts down the dataserver instance.
Update Sybase Version Tag	This step updates the Sybase Instance. Version metadata information for a Sybase Dataserver Instance.
Backout Rolledback Sybase ASE Home	This step backouts the rolled back Sybase ASE home.
Copy Directory	This step takes backup of the Sybase installation folder.
Startup Sybase Servers v2	This step invokes the Sybase commands to startup the Sybase servers. It can startup dataserver, backupserver, and monserver if proper input parameter values are provided. It verifies that the servers have been started successfully by checking the process running on the operating system.
Copy Directory	This step takes backup of the Sybase installation folder.
Startup Sybase Servers v2	This step invokes the Sybase commands to startup the Sybase servers. It can startup dataserver, backupserver, and monserver if proper input parameter values are provided. It verifies that the servers have been started successfully by checking the process running on the operating system.

For parameter descriptions and defaults, see ["Parameters for Sybase - Rollback Patch from Home and Instance" on page 834](#).

How to Run this Workflow

The following instructions show you how to customize and run the Sybase - Rollback from Home and Instance workflow in your environment.

The workflow provides default values for some parameters. These default values are usually sufficient for a "typical" installation. You can override the defaults by specifying parameter values in the deployment. You can also expose additional parameters in the workflow, if necessary, to accomplish more advanced scenarios. Any parameters not explicitly specified in the deployment will have the default values listed in ["Parameters for Sybase - Rollback Patch from Home and Instance" on page 834](#).

Note: Before following this procedure, review the ["Prerequisites for this Workflow" on page 823](#), and ensure that all requirements are satisfied.

To use the Sybase - Rollback from Home and Instance workflow:

1. Create a deployable copy of the workflow.
2. Determine the values that you will specify for the following parameters:

Call Wrapper Parameters

Parameter Name	Default Value	Required	Description
Call Wrapper	see description	required	Command that will execute this step (or subsequent steps) as a specific user. For UNIX targets, the default is: <code>/opt/hp/dma/client/jython.sh</code> running as root
Sybase OS User Name	sybase	required	OS user who owns the Sybase ASE installation directory.

Basic Parameters

Parameter Name	Default Value	Required	Description
Backup Sybase System Databases	Yes	optional	Flag that determines whether to backup Sybase system databases before EBF patch is rolled back. If yes, Sybase system database backup is taken. If no, Sybase system configuration backup is not taken. Valid values are y, yes, true, n, no, or false. Default is yes.
Backup Sybase System Tables	Yes	optional	Flag that determines whether to backup Sybase system tables before EBF patch is rolled back. If yes, Sybase system table backup is taken. If no, Sybase system configuration backup is not taken. Valid values are y, yes, true, n, no, or false. Default is yes.
Sybase Backup Directory to Rollback	no default	required	The fully-qualified backup directory of the Sybase ASE binary files that was created before applying the recent EBF/ESD Patch. Example: <code>/opt/syb_backup/EBF20953/sybase</code>
Sybase Data Directory after Rollback	no default	required	The fully-qualified directory of the Sybase ASE data files that is created after the rollback.
Sybase Installation Backup Directory	no default	required	The directory where the workflow will back up the current (working) Sybase installation directory, important system tables backup, and server configuration backup. Example: <code>opt/sybase/ase_155_backup_20120829</code>

Advanced Parameters

Parameter Name	Default Value	Required	Description
Backup Server Name	no default	optional	The Backup Server name associated with the Adaptive Server (dataserver). Backup Server is responsible for performing backups (dumps) and restores (loads) on selected databases and transaction logs. If not specified, it will not be rebooted after rolling back the patch.
Clean on Failure	no default	optional	Flag that determines whether to clean up on workflow failure. If yes, downloaded files will be cleaned up on failure of workflow. Valid values are y, yes, true, n, no, or false. Default is yes.
Master Device Name	master.dat	optional	Name of the Sybase system device where the master database is mounted and running. If the default device for the master database is not master.dat, it is required. If using raw device provisioning and the master database is mounted on dev/raw/raw1, then the value can be raw1. The default is master.
Monitor Server Name	no default	optional	The Monitor Server name associated with the Adaptive Server (dataserver). Monitor Server is responsible for monitoring and supervising of Adaptive Server. If not specified, it will not be rebooted after rolling back the patch.
Server Errorlog File Format	%s.log	optional	Adaptive Server errorlog file format. Used to allow a non-standard SAP server errorlog file name. Specify your own format that includes '%s'. The '%s' will be replaced with the Adaptive Server name. For example, if set to errorLog_ %s and the server name is 'NY_DS', the workflow will create the errorlog file errorLog_NY_DS. The same convention also applies if any backupserver or monserver are being patched and rebooted. The default is %s.log.
Sybase Installed Home	no default	required	The current Sybase installation directory with absolute path. If

Advanced Parameters, continued

Parameter Name	Default Value	Required	Description
			Discovery was run before executing the current workflow, the default is populated from the SA core. If user wants to specify installation directory other than the one that is discovered, then it can be specified. Example: /opt/sybase.
Sybase Instance Name	no default	required	The current Sybase ASE Server/instance name. If Discovery was run before executing the current workflow, the default is populated from the SA core. If user wants to specify Sybase ASE Instance/Server other than the one that is discovered, then it can be specified. Example: LN_SERVER.
Sybase Instance Password	no default	required	The current Sybase ASE Server/instance login password. If Discovery was run before executing the current workflow, the default is populated from the SA core. If user wants to specify Sybase ASE Instance/Server login password other than the one that is discovered, then it can be specified. Example: PaS#%&Wor*
Sybase Instance User	no default	required	The current Sybase ASE Server/instance login user. If Discovery was run before executing the current workflow, the default is populated from the SA core. If user wants to specify Sybase ASE Instance/Server login user other than the one that is discovered, then it can be specified. Example: sa.
Sybase Post Patch System Script List	installmaster, instmsgs.ebf, installcommit	optional	Comma-separated list of Sybase provided scripts to be run after rolling back the patch from the Sybase instance. These scripts make the appropriate changes to the system tables and procedures and update the Adaptive Server version. The default is 'installmaster, instmsgs.ebf, or installcommit.

3. In the workflow editor, expose any additional parameters that you need. You will specify values for those parameters when you create the deployment.

4. Save the changes to the workflow (click **Save** in the lower right corner).
5. Create a new deployment.
6. On the Parameters tab, specify values for the required parameters listed in step 2. You do not need to specify values for those parameters whose default values are appropriate for your environment.
7. On the Targets tab, specify one or more targets for this deployment.
8. Save the deployment (click **Save** in the lower right corner).
9. Run the workflow using this deployment.

To verify the results:

See the Console page output for error messages that indicate whether problems occurred during the application of the patches. The workflow will complete and report SUCCESS on the Console if it has run successfully. If an error occurs during workflow execution, the error is logged, and the workflow terminates in the FAILURE state.

Optional: If you want to further verify that the patch was successfully applied to the Sybase Database Instances associated with the Sybase Home:

1. Verify the EBF version by querying the global variable (@@version) value. It should match the EBF Patch Number specified.
2. Verify that all databases are online and users are able to log-in.
3. Run basic database consistency check commands, and ensure that no errors are reported.

Sample Scenario

It is very straightforward to run the Sybase - Rollback from Home and Instance workflow. This topic shows you typical parameter values to use.

Input Parameters for "Prepare Sybase Call Wrapper"

Parameter Name	Example Value	Description
Call Wrapper	jython	The command that executes the step as the OS administrative user (for example, <code>sudo su - root /opt/hp/dma/client/bin/jython.sh</code> for UNIX targets)
Sybase OS User Name	sybase	Sybase Account OS user who owns the Sybase ASE installation directory. Workflow steps will switch to Sybase Account user to perform any administrative tasks where Sybase Account User is necessary.

Input Parameters for "Gather Parameters for Rollback Patch from Home and Instance"

Parameter Name	Example Value	Description
Backup Sybase System Databases	yes	Flag that determines whether to backup sybase system databases before EBF patch is applied. If yes, backup sybase system databases will be done before EBF patching. If no, backup sybase system databases will be skipped.
Backup Sybase System Tables	yes	Flag that determines whether to backup sybase system tables before EBF patch is applied. If yes, backup sybase system tables will be done before EBF patching. If no, backup sybase system tables will be skipped.
Sybase Backup Data Directory to Rollback	/opt/app/syb_backup/EBF20953/syb_data	The fully-qualified robust backup directory of the Sybase ASE data files that was created before applying the recent EBF/ESD Patch.
Sybase Backup Directory to Rollback	/opt/app/syb_backup/EBF20953/sybase	The fully-qualified robust backup directory of the Sybase ASE binary files that was created before applying the recent EBF/ESD Patch.
Sybase Data Directory after Rollback	/opt/app/syb_data	The fully-qualified directory of the Sybase ASE data files that is created after rollback.
Sybase Installation Backup Directory	/opt/app/syb_backup/ase_157_backup20150508	The directory where the workflow will back up the current (working) Sybase installation directory, important system tables backup, and server configuration backup.

Input Parameters for "Gather Advanced Parameters for Sybase Rollback from Home and Instance"

Parameter Name	Example Value	Description
Backup server Name	BS_200	The Backup Server name associated with the Adaptive Server ('dataserver'). Backup Server is responsible for performing backups (dumps) and restores (loads) on selected databases and transaction logs. If not specified, it will not be rebooted after rolling back the patch.
Clean on Failure	yes	Flag that determines whether to clean up on workflow failure. If yes, downloaded files will be cleaned up on failure of workflow.

Parameters for Sybase - Rollback Patch from Home and Instance

The following tables describe the required and optional input parameters for this workflow.

Input Parameters for Prepare Sybase Call Wrapper

Parameter Name	Default Value	Required	Description
Call Wrapper	see description	required	Command that will execute this step (or subsequent steps) as a specific user. For UNIX targets, the default is: <code>/opt/hp/dma/client/jython.sh</code> running as root
Sybase OS User Name	sybase	required	OS user who owns the Sybase ASE installation directory.

Input Parameters for Gather Parameters for Rollback Patch Home and Instance

Parameter Name	Default Value	Required	Description
Backup Sybase System Databases	Yes	optional	Flag that determines whether to backup Sybase system databases before EBF patch is rolled back. If yes, Sybase system database backup is taken. If no, Sybase system configuration backup is not taken. Valid values are y, yes, true, n, no, or false. Default is yes.
Backup Sybase System Tables	Yes	optional	Flag that determines whether to backup Sybase system tables before EBF patch is rolled back. If yes, Sybase system table backup is taken. If no, Sybase system configuration backup is not taken. Valid values are y, yes, true, n, no, or false. Default is yes.
Sybase Backup Data Directory to Rollback	no default	required	The fully-qualified backup directory of the Sybase ASE data files that was created before applying the recent EBF/ESD Patch. Example: <code>/opt/syb_backup/EBF20953/syb_data</code>
Sybase Backup Directory to Rollback	no default	required	The fully-qualified backup directory of the Sybase ASE binary files that was created before applying the recent EBF/ESD Patch. Example: <code>/opt/syb_backup/EBF20953/sybase</code>
Sybase Installation Backup Directory	no default	required	The directory where the workflow will back up the current (working) Sybase installation directory, important system tables backup, and server configuration backup. Example: <code>opt/sybase/ase_155_backup_20120829</code>

Additional Input Parameters for Gather Advanced Parameters for Sybase Rollback Home and Instance

Parameter Name	Default Value	Required	Description
Backup Server Name	no default	optional	The Backup Server name associated with the Adaptive Server (dataserver). Backup Server is responsible for performing backups (dumps) and restores (loads) on selected databases and transaction logs. If not specified, it will not be rebooted after rolling back the patch.
Clean on Failure	no default	optional	Flag that determines whether to clean up on workflow failure. If yes, downloaded files will be cleaned up on failure of workflow. Valid values are y, yes, true, n, no, or false. Default is yes.
Master Device Name	master.dat	optional	Name of the Sybase system device where the master database is mounted and running. If the default device for the master database is not master.dat, it is required. If using raw device provisioning and the master database is mounted on dev/raw/raw1, then the value can be raw1. The default is master.
Monitor Server Name	no default	optional	The Monitor Server name associated with the Adaptive Server (dataserver). Monitor Server is responsible for monitoring and supervising of Adaptive Server. If not specified, it will not be rebooted after rolling back the patch.
Server Errorlog File Format	%s.log	optional	Adaptive Server errorlog file format. Used to allow a non-standard SAP server errorlog file name. Specify your own format that includes '%s'. The '%s' will be replaced with the Adaptive Server name. For example, if set to errorLog_%s and the server name is 'NY_DS', the workflow will create the errorlog file errorLog_NY_DS. The same convention also applies if any backupserver or monserver are being patched and rebooted. The default is %s.log.
Sybase Installed Home	no default	required	The current Sybase installation directory with absolute path. If Discovery was run before executing the current workflow, the default is populated from the SA core. If user wants to specify installation directory other than the one that is discovered, then it can be specified. Example: /opt/sybase/.

Additional Input Parameters for Gather Advanced Parameters for Sybase Rollback Home and Instance, continued

Parameter Name	Default Value	Required	Description
Sybase Instance Name	no default	required	The current Sybase ASE Server/instance name. If Discovery was run before executing the current workflow, the default is populated from the SA core. If user wants to specify Sybase ASE Instance/Server other than the one that is discovered, then it can be specified. Example: LN_SERVER.
Sybase Instance Password	no default	required	The current Sybase ASE Server/instance login password. If Discovery was run before executing the current workflow, the default is populated from the SA core. If user wants to specify Sybase ASE Instance/Server login password other than the one that is discovered, then it can be specified. Example: PaS#%&Wor*
Sybase Instance User	no default	required	The current Sybase ASE Server/instance login user. If Discovery was run before executing the current workflow, the default is populated from the SA core. If user wants to specify Sybase ASE Instance/Server login user other than the one that is discovered, then it can be specified. Example: sas.
Sybase Post Patch System Script List	installmaster, instmsgs.ebf, installcommit	optional	Comma-separated list of Sybase provided scripts to be run after rolling back the patch from the Sybase instance. These scripts make the appropriate changes to the system tables and procedures and update the Adaptive Server version. The default is 'installmaster, instmsgs.ebf, or installcommit.

Provision Sybase ASE 15 Server

This workflow installs and configures Sybase Adaptive Server Enterprise (ASE) version 15.0.3 or 15.5 Enterprise Edition.

The workflow performs a “typical” installation using default values for many ASE settings. You can override these default values by either specifying values in the deployment or providing a customized response file. If you choose to not provide a response file, ensure that all required parameters have values.

To use this workflow in your environment, see the following information:

Topic	Information Included
"Prerequisites" below	List of prerequisites that must be satisfied before you can run this workflow
"How this workflow works" on the next page	Information about what the workflow does, including validation checks performed, steps executed, and step descriptions
"How to run this workflow" on page 839	Instructions for running this workflow in your environment
"Parameters for Provision Sybase ASE 15 Server" on page 844	List of input parameters for this workflow

Prerequisites

Before performing the procedures in this section, your environment must meet the following minimum requirements:

- A server running one of the following operating systems:
 - Red Hat Enterprise Linux
 - SUSE Linux Enterprise
 - Solaris (SPARC)
 - AIX

Tip: See the *DMA Support Matrix* for supported operating system versions.

See the Sybase Release Bulletin to verify that the operating system platform is certified for the Sybase version.

- Sufficient disk space on the target servers.
- The user specified for Sybase OS User Name must be a member of the group specified for Default Group.
- Sybase license: You must acquire and activate a valid Sybase license within 30 days of installation. You can either specify the license information by providing values for the pertinent optional parameters, or you can use the SySAM utility to manually activate your license later.
- DMA license
- The Provision Sybase ASE 15 Server workflow must have the unchallenged ability to become the

following:

OS administrator user (typically “root” on UNIX systems)

Sybase database user (typically “sybase”)

Sybase administrator user (typically “sa”)

- The Provision Sybase ASE 15 Server workflow must have access to the ASE installation binaries, either on a network drive or on a DVD (which must be in the DVD drive).
- The infrastructure required for provisioning is in place.
- Shared memory is properly configured.
- The target servers must have the `gunzip` and `tar` utilities in the `$PATH`.
- On Linux or Solaris platforms, the `sudo` package must be installed on the target servers.
- The Configure Sybase ASE 15 Server workflow must have the specified Sybase instance available.
- The Configure Sybase ASE 15 Server workflow must have the Backup Server component associated with this Adaptive Server is running, and the two components can communicate with each other.

Note: For complete installation requirements for SAP Sybase , see:

sybooks.sybase.com/sybooks/sybooks.xhtml

How this workflow works

This workflow performs the following actions:

Installs Sybase Adaptive Server Enterprise (ASE) at the specified location on the target server using silent install method.

Steps Executed

The Provision Sybase ASE 15 Server workflow includes the following steps. Each step must complete successfully before the next step can start. If a step fails, the workflow reports a failure and all subsequent steps are skipped.

Steps used by Provision Sybase ASE 15 Server

Workflow Step	Description
Prepare Sybase Call Wrapper	Prepare the call wrappers needed to become the owner of the Sybase Database software and root.

Steps used by Provision Sybase ASE 15 Server, continued

Workflow Step	Description
Validate Sybase ASE 15 Provisioning Parameters	Sets up all the parameters required to run the Sybase Provision ASE workflow. This step also checks minimum system requirements and disk space.
Sybase - Advanced Parameters	This step sets all the advanced configurable parameters for Provision Sybase ASE 15 Server that are used in subsequent workflow steps.
Setup Sybase Pre-Installation	This steps sets the OS User as the owner of the Sybase related directories.
Uncompress Sybase File	Gets the archive into the specified directory and unpacks it.
Run Sybase Silent Install	Run setup. Install user specified or default configuration for Sybase ASE.
Set Sybase User Password	Set the Sybase ASE database server password at the end of ASE provisioning.
Validate Results	Logon to Sybase ASE database server and validate the system devices and databases are created post provision.

How to run this workflow

The following instructions show you how to customize and run the Provision Sybase ASE 15 Server workflow in your environment.

The workflow provides default values for some parameters. These default values are usually sufficient for a "typical" installation. You can override the defaults by specifying parameter values in the deployment. You can also expose additional parameters in the workflow, if necessary, to accomplish more advanced scenarios. Any parameters not explicitly specified in the deployment will have the default values listed in ["Parameters for Provision Sybase ASE 15 Server" on page 844](#).

Note: Before following this procedure, review the ["Prerequisites" on page 837](#), and ensure that all requirements are satisfied.

To use the Provision Sybase ASE 15 Server workflow:

1. Create a deployable copy of the workflow (see "Create a Deployable Workflow" in *DMA Quick Start Tutorial*)
 - a. Determine the values that you will specify for the following parameters.

The following tables describe the required and optional input parameters for this workflow.

Parameters Defined in this Step: Prepare Sybase Call Wrapper

Parameter Name	Example Value	Description
Call Wrapper	jython	Required: Command that will execute the subsequent steps as the OS administrative user. Example for UNIX targets: <code>sudo su - root /opt/hp/dma/client/bin/ jython.sh</code>
Sybase OS User Name	sybase	Required: The OS user who owns the Sybase ASE installation directory. This is the directory specified in the Sybase Install Directory parameter, where the Sybase ASE binaries will be extracted.

Step: Sybase - Advanced Parameters

Parameter	Description	Example Value
Backup Server Name	Required (if a response file not used): The Backup Server name. The backup server is responsible for performing backups (dumps) and restores (loads) on selected databases and transaction logs. The default is based on the Sybase ASE version.	NY_DSMIN2_BS
Database Server Name	Required (if a response file not used): The Adaptive Server name. The Adaptive server component manages databases and users, records the location of data on disks, maps logical data descriptions to physical data storage, and manages data and procedure caches in memory. The default is based on the Sybase ASE version.	NY_DSMIN2
File To Download	Required: File name of the compressed Sybase ASE installation binary. The default is based on the Sybase ASE version and the target operating system. For example: <code>ase155esd2_linuxx86-64.tgz</code>	<code>ase155esd2_linuxx86-64.tgz</code>
Master Device	Optional for file system installation, required for raw partition installation: For a file system installation, this is the file system location (absolute path) where the Sybase ASE master device will	

Step: Sybase - Advanced Parameters, continued

Parameter	Description	Example Value
	<p>reside. If you do not specify this path, a default path will be used (\$SYBASE/\$SYBASE_ASE/data).</p> <p>For a raw partition installation, this is the name of the bound raw device where the Sybase ASE master device will be mounted. For example: /dev/raw/raw1 on Linux or /dev/rdisk/c0t10d0s0 on Solaris</p>	
Master Device Size	Optional: Size (in MB) of the master device. Minimum recommended size is 240 MB. For a file system installation, the maximum amount of space initially allocated for the master device (can be increased later, if necessary). The default is the server page size. The default is 200.	
Raw Device File	<p>Optional: The system raw device binding file (required to create databases on raw bound devices). This file maps raw partitions to character devices. The raw devices listed in this file must be created and started prior to running this workflow. This parameter value is populated automatically by DMA.</p> <p>For example: /etc/sysconfig/rawdevices on Linux. The value should be empty for Solaris raw device provisioning.</p>	
Sybase ASE Version	Required: The version of Sybase ASE that you are installing (for example: 15.7, 15.5 or 15.0.3).	15.5
System Device	<p>Optional for file system installation, required for raw partition installation: For a file system installation, this is the file system location (absolute path) where the Sybase ASEsybsystemdb device will reside. If you do not specify this path, a default path based on the Sybase Install Directory will be used (\$SYBASE/data).</p> <p>For a raw partition installation, this is the name of the bound raw device where the Sybase</p>	

Step: Sybase - Advanced Parameters, continued

Parameter	Description	Example Value
	ASEsybsystemdb device will be mounted. For example: /dev/raw/raw2 on Linux, /dev/rdisk/c0t10d0s1 on Solaris	
System Device Size	<p>Optional for file system installation, required for raw partition installation: Maximum amount of space that will be initially allocated for the sybsystemdb device (in MB). It can be increased later, if necessary. The default is 50.</p> <p>For a raw partition installation, this must be less than or equal to the size of the raw partition. The device can be resized later, but the partition cannot be.</p> <p>Minimum recommended size: 5-24 MB (larger page sizes require more space).</p>	
System Proc Device	<p>Optional for file system installation, required for raw partition installation: For a file system installation, this is the file system location (absolute path) where the Sybase ASEsysprocsdev device will reside. If you do not specify this path, a default path based on the Sybase Install Directory will be used (\$SYBASE/data).</p> <p>For a raw partition installation, this is the name of the bound raw device where the Sybase ASEsysprocsdev device will be mounted. For example: /dev/raw/raw3 on Linux or /dev/rdisk/c0t10d0s2 on Solaris</p>	
System Proc Device Size	<p>Optional for file system installation, required for raw partition installation: Maximum amount of space that will be initially allocated for the sysprocsdev device (in MB). It can be increased later, if necessary.</p> <p>If you do not provide a value for a file system installation 200 MB is used.</p> <p>For a raw partition installation, this</p>	

Step: Sybase - Advanced Parameters, continued

Parameter	Description	Example Value
	<p>must be less than or equal to the size of the raw partition. The device can be resized later, but the partition cannot be.</p> <p>Minimum recommended size: 140 MB</p>	
Temp DB Device	<p>Optional for file system installation, required for raw partition installation: For a file system installation, this is the file system location (absolute path) where the Sybase ASE<code>tempdbdev</code> device will reside (for example: <code>\$SYBASE/data</code>). If you do not specify this path, a default path based on the Sybase Install Directory will be used.</p> <p>For a raw partition installation, this is the name of the bound raw device where the Sybase ASE<code>sybtempdb</code> device will be mounted. For example: <code>/dev/raw/raw4</code> on Linux or <code>/dev/rdisk/c0t10d0s4</code> on Solaris</p>	
Temp DB Device Size	<p>Optional for file system installation, required for raw partition installation: Maximum amount of space that will be initially allocated for the <code>tempdbdev</code> device (in MB). It can be increased later, if necessary. The default is 100.</p> <p>For a raw partition installation, this must be less than or equal to the size of the raw partition. The device can be resized later, but the partition cannot be.</p> <p>Minimum recommended size: 5 \u2013 24MB (larger page sizes require more space).</p>	

2. In the workflow editor, expose any additional parameters that you need. You will specify values for those parameters when you create the deployment or at runtime.
3. Save the changes to the workflow (click **Save** in the lower right corner).
4. Create a new deployment. See "Create a Deployment" in *DMA Quick Start Tutorial* for instructions.

5. On the Parameters tab, specify values (or set the type to Runtime Value) for the required parameters listed in step 2 and any additional parameters that you have exposed. You do not need to specify values for those parameters whose default values are appropriate for your environment.
6. On the Targets tab, specify one or more targets for this deployment.
7. Save the deployment (click **Save** in the lower right corner).
8. Run the workflow using this deployment, specifying any runtime parameters. See "Run Your Workflow" in (*DMA Quick Start Tutorial* for instructions.

To verify the results:

The workflow will complete and report SUCCESS on the Console if it has run successfully. If an error occurs during workflow execution, the error is logged, and the workflow terminates in the FAILURE state.

Parameters for Provision Sybase ASE 15 Server

The following tables describe the required and optional input parameters for this workflow.

Parameters Defined in this Step: Prepare Sybase Call Wrapper

Parameter Name	Required	Example Value	Description
Call Wrapper	required	jython	Required: Command that will execute the subsequent steps as the OS administrative user. Example for UNIX targets: sudo su - root /opt/hp/dma/client/bin/ jython.sh
Sybase OS User Name	required	sybase	Required: The OS user who owns the Sybase ASE installation directory. This is the directory specified in the Sybase Install Directory parameter, where the Sybase ASE binaries will be extracted.

Step: Sybase - Advanced Parameters

Parameter	Required	Example Value	Description
Backup Server Name	required	NY_DSMIN2_BS	Required (if a response file not used): The Backup Server name. The backup server is responsible for performing backups (dumps) and restores (loads) on selected databases and transaction logs. The default is based on the Sybase ASE version.

Step: Sybase - Advanced Parameters, continued

Parameter	Required	Example Value	Description
Database Server Name	required	NY_DSMIN2	<p>Required (if a response file not used): The Adaptive Server name. The Adaptive server component manages databases and users, records the location of data on disks, maps logical data descriptions to physical data storage, and manages data and procedure caches in memory.</p> <p>The default is based on the Sybase ASE version.</p>
File To Download	required	ase155esd2_linuxx86-64.tgz	<p>Required: File name of the compressed Sybase ASE installation binary.</p> <p>The default is based on the Sybase ASE version and the target operating system.</p> <p>For example: ase155esd2_linuxx86-64.tgz</p>
Master Device	optional		<p>Optional for file system installation, required for raw partition installation: For a file system installation, this is the file system location (absolute path) where the Sybase ASE master device will reside. If you do not specify this path, a default path will be used (\$SYBASE/\$SYBASE_ASE/data).</p> <p>For a raw partition installation, this is the name of the bound raw device where the Sybase ASE master device will be mounted. For example: /dev/raw/raw1 on Linux or /dev/rdisk/c0t10d0s0 on Solaris</p>
Master Device Size	optional		<p>Optional: Size (in MB) of the master device. Minimum recommended size is 240 MB. For a file system installation, the maximum amount of space initially allocated for the master device (can be increased later, if necessary). The default is the server page size. The default is 200.</p>
Raw Device File	optional		<p>Optional: The system raw device binding file (required to create databases on raw bound devices). This file maps raw partitions to character devices. The raw devices listed in this file must be created</p>

Step: Sybase - Advanced Parameters, continued

Parameter	Required	Example Value	Description
			and started prior to running this workflow. This parameter value is populated automatically by DMA. For example: /etc/sysconfig/rawdevices on Linux. The value should be empty for Solaris raw device provisioning.
Sybase ASE Version	required	15.5	Required: The version of Sybase ASE that you are installing (for example: 15.7, 15.5 or 15.0.3).
System Device	optional		Optional for file system installation, required for raw partition installation: For a file system installation, this is the file system location (absolute path) where the Sybase ASEsybsystemdb device will reside. If you do not specify this path, a default path based on the Sybase Install Directory will be used (\$SYBASE/data). For a raw partition installation, this is the name of the bound raw device where the Sybase ASEsybsystemdb device will be mounted. For example: /dev/raw/raw2 on Linux, /dev/rdisk/c0t10d0s1 on Solaris
System Device Size	optional		Optional for file system installation, required for raw partition installation: Maximum amount of space that will be initially allocated for the sybsystemdb device (in MB). It can be increased later, if necessary. The default is 50. For a raw partition installation, this must be less than or equal to the size of the raw partition. The device can be resized later, but the partition cannot be. Minimum recommended size: 5-24 MB (larger page sizes require more space).
System Proc Device	optional		Optional for file system installation, required for raw partition installation: For a file system installation, this is the file system location (absolute path) where the Sybase ASEsysprocsdev device will reside. If you do not specify this path, a default path based on the

Step: Sybase - Advanced Parameters, continued

Parameter	Required	Example Value	Description
			<p>Sybase Install Directory will be used (\$SYBASE/data).</p> <p>For a raw partition installation, this is the name of the bound raw device where the Sybase ASEsysprocsdev device will be mounted. For example: /dev/raw/raw3 on Linux or /dev/rdisk/c0t10d0s2 on Solaris</p>
System Proc Device Size	optional		<p>Optional for file system installation, required for raw partition installation: Maximum amount of space that will be initially allocated for the sysprocsdev device (in MB). It can be increased later, if necessary.</p> <p>If you do not provide a value for a file system installation 200 MB is used.</p> <p>For a raw partition installation, this must be less than or equal to the size of the raw partition. The device can be resized later, but the partition cannot be.</p> <p>Minimum recommended size: 140 MB</p>
Temp DB Device	optional		<p>Optional for file system installation, required for raw partition installation: For a file system installation, this is the file system location (absolute path) where the Sybase ASEtempdbdev device will reside (for example: \$SYBASE/data). If you do not specify this path, a default path based on the Sybase Install Directory will be used.</p> <p>For a raw partition installation, this is the name of the bound raw device where the Sybase ASEsybtempdb device will be mounted. For example: /dev/raw/raw4 on Linux or /dev/rdisk/c0t10d0s4 on Solaris</p>
Temp DB Device Size	optional		<p>Optional for file system installation, required for raw partition installation: Maximum amount of space that will be initially allocated for the tempdbdev device (in MB). It can be increased later, if</p>

Step: Sybase - Advanced Parameters, continued

Parameter	Required	Example Value	Description
			<p>necessary. The default is 100.</p> <p>For a raw partition installation, this must be less than or equal to the size of the raw partition. The device can be resized later, but the partition cannot be.</p> <p>Minimum recommended size: 5 \u2013 24MB (larger page sizes require more space).</p>

Configure Sybase ASE 15 Server

This workflow enables you to configure a large number of user-definable parameter value settings for an existing Sybase Adaptive Server Enterprise (ASE) version 15 instance. You can use these settings to control how the Adaptive Server behaves and optimize its performance. The workflow updates settings for both static and dynamic parameters. When static parameters are updated, the workflow automatically restarts the Adaptive Server.

To use this workflow in your environment, see the following information:

Topic	Information Included
"Prerequisites" below	List of prerequisites that must be satisfied before you can run this workflow
"How this workflow works" on page 850	Information about what the workflow does, including validation checks performed, steps executed, and step descriptions
"How to run this workflow" on page 851	Instructions for running this workflow in your environment
"Parameters for Configure Sybase ASE 15 Server" on page 853	List of input parameters for this workflow

Prerequisites

Before performing the procedures in this section, your environment must meet the following minimum requirements:

- A server running one of the following operating systems:

- Red Hat Enterprise Linux
- SUSE Linux Enterprise
- Solaris (SPARC)
- AIX

Tip: See the *DMA Support Matrix* for supported operating system versions.

See the Sybase Release Bulletin to verify that the operating system platform is certified for the Sybase version.

- Sufficient disk space on the target servers.
- The user specified for Sybase OS User Name must be a member of the group specified for Default Group.
- Sybase license: You must acquire and activate a valid Sybase license within 30 days of installation. You can either specify the license information by providing values for the pertinent optional parameters, or you can use the SySAM utility to manually activate your license later.
- DMA license
- The Provision Sybase ASE 15 Server workflow must have the unchallenged ability to become the following:
 - OS administrator user (typically “root” on UNIX systems)
 - Sybase database user (typically “sybase”)
 - Sybase administrator user (typically “sa”)
- The Provision Sybase ASE 15 Server workflow must have access to the ASE installation binaries, either on a network drive or on a DVD (which must be in the DVD drive).
- The infrastructure required for provisioning is in place.
- Shared memory is properly configured.
- The target servers must have the `gunzip` and `tar` utilities in the `$PATH`.
- On Linux or Solaris platforms, the `sudo` package must be installed on the target servers.
- The Configure Sybase ASE 15 Server workflow must have the specified Sybase instance available.

- The Configure Sybase ASE 15 Server workflow must have the Backup Server component associated with this Adaptive Server is running, and the two components can communicate with each other.

Note: For complete installation requirements for SAP Sybase , see:

sybooks.sybase.com/sybooks/sybooks.xhtml

How this workflow works

This workflow performs the following actions:

Configures Sybase Adaptive Server Enterprise (ASE) at the specified location on the target server using silent install method.

Steps Executed

The Configure Sybase ASE 15 Server workflow includes the following steps. Each step must complete successfully before the next step can start. If a step fails, the workflow reports a failure and all subsequent steps are skipped.

Steps used by Provision Sybase ASE 15 Server

Workflow Step	Description
Prepare Sybase Call Wrapper	Prepare the call wrappers needed to become the owner of the Sybase Database software and root.
Gather Sybase ASE 15 Server Configuration Parameters	Accepts and outputs the basic parameters for Sybase Server Configurations
Gather Advanced Sybase ASE 15 Server Configuration Parameters	Accepts advanced Server Configuration parameters and handles defaulting for those parameters which are hidden. Transforms parameter values into formats suitable for passing to other steps.
Validate Sybase Database Instance	Accepts the user inputs and validates the Sybase ASE server is up and running and be able to communicate with backup server.
Configure Sybase ASE 15 Server Parameter Options	Runs the ASE Server Configuration System stored procedure and configure the behavior of server by setting the values for option parameters.
Shutdown Sybase Dataserver	The Dataserver instance must be shutdown prior to installing the EBF patch.
Startup Sybase Dataserver	Starts up the Dataserver instance.
Validate Configure Sybase ASE 15 Server	Post Validation of Sybase ASE 15 Server Configuration

How to run this workflow

The following instructions show you how to customize and run the Configure Sybase ASE 15 Server workflow in your environment.

The workflow provides default values for some parameters. These default values are usually sufficient for a "typical" installation. You can override the defaults by specifying parameter values in the deployment. You can also expose additional parameters in the workflow, if necessary, to accomplish more advanced scenarios. Any parameters not explicitly specified in the deployment will have the default values listed in ["Parameters for Configure Sybase ASE 15 Server" on page 853](#).

Note: Before following this procedure, review the ["Prerequisites" on page 848](#), and ensure that all requirements are satisfied.

To use the Configure Sybase ASE 15 Server workflow:

1. Create a deployable copy of the workflow (see "Create a Deployable Workflow" in *DMA Quick Start Tutorial*)
 - a. Determine the values that you will specify for the following parameters.

The following tables describe the required and optional input parameters for this workflow.

Parameters Defined in this Step: Prepare Sybase Call Wrapper

Parameter Name	Example Value	Description
Call Wrapper	jython	Required: Command that will execute the subsequent steps as the OS administrative user. Example for UNIX targets: sudo su - root /opt/hp/dma/client/bin/ jython.sh
Sybase OS User Name	sybase	Required: The OS user who owns the Sybase ASE installation directory. This is the directory specified in the Sybase Install Directory parameter, where the Sybase ASE binaries will be extracted.

Step: Gather Sybase ASE 15 Server Configuration Parameters

Parameter	Description	Example Value
ASE SysAdmin Password	Required: Password for ASE SysAdmin Password.	●●●
ASE SysAdmin Username	Required: Sybase database username that will perform the restore.	sa
Call Wrapper	jython	Required: Command that will execute the subsequent steps as

Step: Gather Sybase ASE 15 Server Configuration Parameters, continued

Parameter	Description	Example Value
		the OS administrative user. Example for UNIX targets: sudo su - root /opt/hp/dma/client/bin/ jython.sh
Database Instance Name	Required: The Sybase ASE Database Instance Name.	NY_DSMIN7
Sybase ASE Home Directory	Required: The Sybase ASE home directory.	/opt/sybase/ASE_15_5

Step: Gather Advanced Sybase ASE 15 Server Configuration Parameters

Parameter	Description	Example Value
Call Wrapper	jython	Required: Command that will execute the subsequent steps as the OS administrative user. Example for UNIX targets: sudo su - root /opt/hp/dma/client/bin/ jython.sh
Configuration Type	Optional: The ASE Server Configuration type. Valid values: Production, Developer, Staging. The default is: Production, Development, Staging	Production, Development, Staging Development

- In the workflow editor, expose any additional parameters that you need. You will specify values for those parameters when you create the deployment or at runtime.
- Save the changes to the workflow (click **Save** in the lower right corner).
- Create a new deployment. See "Create a Deployment" in *DMA Quick Start Tutorial* for instructions.
- On the Parameters tab, specify values (or set the type to Runtime Value) for the required parameters listed in step 2 and any additional parameters that you have exposed. You do not need to specify values for those parameters whose default values are appropriate for your environment.
- On the Targets tab, specify one or more targets for this deployment.
- Save the deployment (click **Save** in the lower right corner).
- Run the workflow using this deployment, specifying any runtime parameters. See "Run Your Workflow" in (*DMA Quick Start Tutorial* for instructions.

To verify the results:

The workflow will complete and report SUCCESS on the Console if it has run successfully. If an error occurs during workflow execution, the error is logged, and the workflow terminates in the FAILURE state.

Parameters for Configure Sybase ASE 15 Server

The following tables describe the required and optional input parameters for this workflow.

Parameters Defined in this Step: Prepare Sybase Call Wrapper

Parameter Name	Required	Example Value	Description
Call Wrapper	required	jython	Required: Command that will execute the subsequent steps as the OS administrative user. Example for UNIX targets: <code>sudo su - root /opt/hp/dma/client/bin/ jython.sh</code>
Sybase OS User Name	required	sybase	Required: The OS user who owns the Sybase ASE installation directory. This is the directory specified in the Sybase Install Directory parameter, where the Sybase ASE binaries will be extracted.

Step: Gather Sybase ASE 15 Server Configuration Parameters

Parameter	Required	Example Value	Description
ASE SysAdmin Password	required	●●●	Required: Password for ASE SysAdmin Password.
ASE SysAdmin Username	required	sa	Required: Sybase database username that will perform the restore.
Call Wrapper	required	Required: Command that will execute the subsequent steps as the OS administrative user. Example for UNIX targets: <code>sudo su - root /opt/hp/dma/client/bin/ jython.sh</code>	jython
Database Instance Name	required	NY_DSMIN7	Required: The Sybase ASE Database Instance Name.
Sybase ASE Home Directory	required	/opt/sybase/ASE_15_5	Required: The Sybase ASE home directory.

Step: Gather Advanced Sybase ASE 15 Server Configuration Parameters

Parameter	Required	Example Value	Description
Call Wrapper	required	Required: Command that will execute the subsequent steps as the OS administrative user. Example for UNIX targets: sudo su - root /opt/hp/dma/client/bin/ jython.sh	jython
Configuration Type	optional	Production, Development, Staging Development	Optional: The ASE Server Configuration type. Valid values: Production, Developer, Staging. The default is: Production, Development, Staging

Create Sybase Database

This workflow initializes Sybase devices and creates a database on a server where Sybase Adaptive Server Enterprise (Sybase ASE) version 15.0.3 or 15.5 is installed and configured. It works at the instance level and supports both file system and raw device installations.

To use this workflow in your environment, see the following information:

Topic	Information Included
"Prerequisites" below	List of prerequisites that must be satisfied before you can run this workflow
"How this workflow works" on page 856	Information about what the workflow does, including validation checks performed, steps executed, and step descriptions
"How to run this workflow" on page 856	Instructions for running this workflow in your environment
"Parameters for Create Sybase Database" on page 859	List of input parameters for this workflow

Prerequisites

Before performing the procedures in this section, your environment must meet the following minimum requirements:

- A server running one of the following operating systems:

- Red Hat Enterprise Linux
- SUSE Linux Enterprise
- Solaris (SPARC)
- AIX

Tip: See the *DMA Support Matrix* for supported operating system versions.

See the Sybase Release Bulletin to verify that the operating system platform is certified for the Sybase version.

- Sufficient disk space on the target servers.
- The user specified for Sybase OS User Name must be a member of the group specified for Default Group.
- Sybase license: You must acquire and activate a valid Sybase license within 30 days of installation. You can either specify the license information by providing values for the pertinent optional parameters, or you can use the SySAM utility to manually activate your license later.
- DMA license
- The Provision Sybase ASE 15 Server workflow must have the unchallenged ability to become the following:
 - OS administrator user (typically “root” on UNIX systems)
 - Sybase database user (typically “sybase”)
 - Sybase administrator user (typically “sa”)
- The Provision Sybase ASE 15 Server workflow must have access to the ASE installation binaries, either on a network drive or on a DVD (which must be in the DVD drive).
- The infrastructure required for provisioning is in place.
- Shared memory is properly configured.
- The target servers must have the `gunzip` and `tar` utilities in the `$PATH`.
- On Linux or Solaris platforms, the `sudo` package must be installed on the target servers.
- The Configure Sybase ASE 15 Server workflow must have the specified Sybase instance available.

- The Configure Sybase ASE 15 Server workflow must have the Backup Server component associated with this Adaptive Server is running, and the two components can communicate with each other.

Note: For complete installation requirements for SAP Sybase , see:

sybooks.sybase.com/sybooks/sybooks.xhtml

How this workflow works

This workflow performs the following actions:

Creates a database where Sybase Adaptive Server Enterprise (ASE) is installed at the specified location on the target server using silent install method.

Steps Executed

The Create Sybase Database workflow includes the following steps. Each step must complete successfully before the next step can start. If a step fails, the workflow reports a failure and all subsequent steps are skipped.

Steps used by Provision Sybase ASE 15 Server

Workflow Step	Description
Prepare Sybase Call Wrapper	Prepare the call wrappers needed to become the owner of the Sybase database software and root.
Validate Sybase Create Database Parameters	Validates Parameters prior to executing the rest of the workflow.
Initialize Sybase Devices	This step initializes the Sybase database devices.
Create Sybase Database	This step creates the Sybase database.

How to run this workflow

The following instructions show you how to customize and run the Create Sybase Database workflow in your environment.

The workflow provides default values for some parameters. These default values are usually sufficient for a "typical" installation. You can override the defaults by specifying parameter values in the deployment. You can also expose additional parameters in the workflow, if necessary, to accomplish more advanced scenarios. Any parameters not explicitly specified in the deployment will have the default values listed in ["Parameters for Create Sybase Database" on page 859](#).

Note: Before following this procedure, review the ["Prerequisites" on page 854](#), and ensure that all requirements are satisfied.

To use the Create Sybase Database workflow:

1. Create a deployable copy of the workflow (see "Create a Deployable Workflow" in *DMA Quick Start Tutorial*)
 - a. Determine the values that you will specify for the following parameters.

The following tables describe the required and optional input parameters for this workflow.

Parameters Defined in this Step: Prepare Sybase Call Wrapper

Parameter Name	Example Value	Description
Call Wrapper	jython	Required: Command that will execute the subsequent steps as the OS administrative user. Example for UNIX targets: <code>sudo su - root /opt/hp/dma/client/bin/ jython.sh</code>
Sybase OS User Name	sybase	Required: The OS user who owns the Sybase ASE installation directory. This is the directory specified in the Sybase Install Directory parameter, where the Sybase ASE binaries will be extracted.

Step: Validate Sybase Create Database Parameters

Parameter	Description	Example Value
Call Wrapper	jython	Required: Command that will execute the subsequent steps as the OS administrative user. Example for UNIX targets: <code>sudo su - root /opt/hp/dma/client/bin/ jython.sh</code>
Create Devices	Required: Flag to determine whether to create devices. If False, devices will not be created. Valid values: True or False	True
Data Device Size	Required for file-based provisioning (filesystem device path), optional for raw devices: Size of Data Device file in megabytes. Partition cannot be shared with other Sybase ASE devices	100
Database Name	Required: Name of the new database.	mydbMIN2
Database Server Name	Required: Name of database server instance where you want to create the new database.	NY_DSMIN2 <i>Use the same value as the Database Server Name parameter for the Provision Sybase ASE 15</i>

Step: Validate Sybase Create Database Parameters, continued

Parameter	Description	Example Value
		<i>Server deployment.</i>
Database Size	Required: Size of the database (megabytes).	5
Disk Sync Flag	Required: Flag that determines whether the disk will be synchronized. If False, 'dsync = false' option is set on disk initializations. Disk writes will be buffered by OS. Valid values: True or False	True
Log Device Size	Required for raw provisioning, optional for file provisioning: Size of log device (megabytes). Partition cannot be shared with other Sybase ASE	10
Logical Data Device Name	Required: The logical data device name that will refer to the physical data device name.	datadev
Logical Log Device Name	Required: The logical log device name that will refer to the physical log device name.	logdev
Physical Data Device Path	Required: If used for provisioning for raw devices, the character raw partition path. For example: /dev/raw/raw1 If used for file system provisioning, the file system device path. For example: /home/sybase/ASE_15/data/my_test_data.dat	/home/sybase/data/data_dev.dat
Physical Log Device Path	Required: If used for raw device provisioning, the character raw partition path. For example: /dev/raw/raw1 If used for file system provisioning, the file system device path. For example: \$SYBASE/\$SYBASE_ASE/data/mytesdevt.dat	/home/sybase/data/log_dev.dat
Sybase Home	Required: The Sybase ASE installation home directory where the database will be created.	/opt/sybase/ASE_15_5 <i>Use the same value as the Sybase ASE Home Directory parameter for the Configure Sybase ASE 15 Server deployment.</i>
Sybase User	Required: The ASE database	sa

Step: Validate Sybase Create Database Parameters, continued

Parameter	Description	Example Value
Name	username for administrative operations. Usually 'sa'.	autotest <i>Use the same value as the ASE SysAdmin Username parameter for the Configure Sybase ASE 15 Server deployment.</i>
Sybase User Password	Required: The password for Sybase User Name.	●●● <i>Use the same value as the ASE SysAdmin Password parameter for the Configure Sybase ASE 15 Server deployment.</i>
Temporary Database	Required: Flag to determine whether the database will be created using the temporary flag. Valid values: 'True' or 'False'	False

2. In the workflow editor, expose any additional parameters that you need. You will specify values for those parameters when you create the deployment or at runtime.
3. Save the changes to the workflow (click **Save** in the lower right corner).
4. Create a new deployment. See "Create a Deployment" in *DMA Quick Start Tutorial* for instructions.
5. On the Parameters tab, specify values (or set the type to Runtime Value) for the required parameters listed in step 2 and any additional parameters that you have exposed. You do not need to specify values for those parameters whose default values are appropriate for your environment.
6. On the Targets tab, specify one or more targets for this deployment.
7. Save the deployment (click **Save** in the lower right corner).
8. Run the workflow using this deployment, specifying any runtime parameters. See "Run Your Workflow" in (*DMA Quick Start Tutorial* for instructions.

To verify the results:

The workflow will complete and report SUCCESS on the Console if it has run successfully. If an error occurs during workflow execution, the error is logged, and the workflow terminates in the FAILURE state.

Parameters for Create Sybase Database

The following tables describe the required and optional input parameters for this workflow.

Parameters Defined in this Step: Prepare Sybase Call Wrapper

Parameter Name	Required	Example Value	Description
Call Wrapper	required	jython	Required: Command that will execute the subsequent steps as the OS administrative user. Example for UNIX targets: sudo su - root /opt/hp/dma/client/bin/ jython.sh
Sybase OS User Name	required	sybase	Required: The OS user who owns the Sybase ASE installation directory. This is the directory specified in the Sybase Install Directory parameter, where the Sybase ASE binaries will be extracted.

Step: Validate Sybase Create Database Parameters

Parameter	Required	Example Value	Description
Create Devices	required	True	Required: Flag to determine whether to create devices. If False, devices will not be created. Valid values: True or False
Data Device Size	required	100	Required for file-based provisioning (filesystem device path), optional for raw devices: Size of Data Device file in megabytes. Partition cannot be shared with other Sybase ASE devices
Database Name	required	mydbMIN2	Required: Name of the new database.
Database Server Name	required	NY_DSMIN2 <i>Use the same value as the Database Server Name parameter for the Provision Sybase ASE 15 Server deployment.</i>	Required: Name of database server instance where you want to create the new database.
Database Size	required	5	Required: Size of the database (megabytes).
Disk Sync Flag	required	True	Required: Flag that determines whether the disk will be synchronized. If False, 'dsync = false' option is set on disk initializations. Disk writes will be buffered by OS. Valid values: True or False
Log Device Size	required	10	Required for raw provisioning, optional for file provisioning: Size of log device (megabytes). Partition cannot be shared with other Sybase ASE

Step: Validate Sybase Create Database Parameters, continued

Parameter	Required	Example Value	Description
Logical Data Device Name	required	datadev	Required: The logical data device name that will refer to the physical data device name.
Logical Log Device Name	required	logdev	Required: The logical log device name that will refer to the physical log device name.
Physical Data Device Path	required	/home/sybase/data/data_dev.dat	Required: If used for provisioning for raw devices, the character raw partition path. For example: /dev/raw/raw1 If used for file system provisioning, the file system device path. For example: /home/sybase/ASE_15/data/my_test_data.dat
Physical Log Device Path	required	/home/sybase/data/log_dev.dat	Required: If used for raw device provisioning, the character raw partition path. For example: /dev/raw/raw1 If used for file system provisioning, the file system device path. For example: \$SYBASE/\$SYBASE_ASE/data/mytesdevt.dat
Sybase Home	required	/opt/sybase/ASE_15_5 <i>Use the same value as the Sybase ASE Home Directory parameter for the Configure Sybase ASE 15 Server deployment.</i>	Required: The Sybase ASE installation home directory where the database will be created.
Sybase User Name	required	sa autotest <i>Use the same value as the ASE SysAdmin Username parameter for the Configure Sybase ASE 15 Server deployment.</i>	Required: The ASE database username for administrative operations. Usually 'sa'.
Sybase User Password	required	●●● <i>Use the same value as the ASE SysAdmin Password parameter for the Configure Sybase ASE 15 Server deployment.</i>	Required: The password for Sybase User Name.
Temporary Database	required	False	Required: Flag to determine whether the database will be created using the temporary flag. Valid values: 'True' or 'False'

Apache Web Server

This section contains the following topics:

Workflow type	Workflow name
Provisioning	"Apache - Provision Software" on the next page

Apache - Provision Software

This workflow does the following:

- deploy an Apache web server archive to a specified location.
- provision new Apache instances. The new instances will be pointing to the deployed Apache Web Server location.
- upgrade/patch existing Apache instances. The existing instances will be pointing to the deployed Apache Web Server location.

This workflow provisions Apache web server versions 2.2.x and 2.4.x. The upgrade/patch is supported within the same version family, for example, 2.2 to 2.2.x.

This Workflow requires a compressed file (.zip or tar.gz). For Windows OS, it should be a .zip file.

The workflow can create multiple Apache instances (new) and upgrade/patch multiple Apache instances (existing). Content root directory corresponds to the instance location of an Apache server installation.

The newly provisioned instances will have the configuration files copied from a deployed Apache Web Server location. Also a copy of the htdocs and cgi content will be copied to the content home of the newly created instances.

Topic	Information Included
"Prerequisites for this workflow"	List of prerequisites that must be satisfied before you can run this workflow
"How this workflow works"	Information about what the workflow does, including validation checks performed, steps executed, and a high-level process flow
"How to Run this Workflow"	Instructions for running this workflow in your environment
"Sample Scenarios"	Examples of typical parameter values for this workflow
"Parameters for Apache - Provision Software"	List of input parameters for this workflow

The process of deploying and running this workflow is the same for all scenarios, but the parameters required will differ depending on the specific scenario that you are implementing.

The workflow provides default values for most parameters. These default values are usually sufficient for a typical provisioning scenario. You can override the defaults by specifying parameter values in the deployment. You can also expose additional parameters in the workflow, if necessary, to accomplish more advanced scenarios.

Any parameters not explicitly specified in the deployment will have the default values listed in ["Parameters for Apache - Provision Software"](#).

Note: For information about the steps in this workflow, see the ["How this workflow works"](#) on [page 867](#).

Note: The documentation for this workflow contains steps that are referred to by their base names. The names in the DMA user interface may have a version appended, for example, v2.

Prerequisites for this workflow

The following prerequisites must be satisfied before you can run the Apache - Provision Software workflow:

- The workflow requires unchallenged `sudo` access to a user (typically root) who can access all required files and directories.

For information about prerequisites for Apache HTTP Server, refer to the [Apache HTTP Server Documentation](#).

How this workflow works

This topic contains the following information about the Apache - Provision Software workflow:

Validation Checks Performed

The workflow checks the following things prior to extracting the binaries. If any of these checks fails, the workflow fails.

1. All required parameters have values. If any required parameter does not have a value—either a value that you specify or a default value—the workflow fails.
2. Directories and host names are valid. No illegal characters are included. The fully qualified path specified for downloading Apache web server binaries exists: `/example/downloads/`.
3. The additional packages that are used by the deployment package must be installed on the target system.
4. The operating system is a supported platform.
5. Sufficient disk space is available to extract the binary files from the compressed archive.
6. Sufficient disk space is available to install Apache web server.

Steps Executed

The Apache - Provision Software workflow includes the following steps. Each step must complete successfully before the next step can start. If a step fails, the workflow reports a failure, and subsequent steps are skipped.

Process Flow

This workflow performs the following tasks:

1. Gathers mandatory and optional input parameters (user-provided) to provision Apache web server.
2. Validates the parameters needed to provision Apache web server.
3. Checks for the existence of a file before downloading.
4. Automates the transfer of files. Verifies checksum of each file transferred.
5. Installs the supported binary files.
6. Extracts the Apache web server archive to the specified directories.
7. Creates and configures new Apache web server instances.
8. Configures existing Apache web server instances.
9. Starts the HTTP server.
10. Tests the installation.
11. Creates Apache services for UNIX.
12. Discovers Apache web server.
13. Gathers files and cleans up.
14. Cleans up downloaded files that are no longer required, based on user-specified flags, in the event of workflow success or failure.

How to Run this Workflow

This topic explains how to customize and run the Tomcat - Provision Software workflow in your environment.

Note: Prior to running this workflow, review the ["Prerequisites for this workflow"](#), and ensure that all requirements are satisfied.

To customize and run the Apache - Provision Software workflow:

1. Create a deployable copy of the workflow.
2. Determine the values that you will specify for the following parameters. These are the parameters that are visible in the deployment by default.

Parameters in the step: Gather Parameters for Apache Provision Software

Parameter Name	Default Value	Description
Apache Group	no default	The user-group that the Apache server will run under Example: apachegrp. The group will be created if it is not already present
Apache Instances	no default	Comma separated list of absolute path to instance locations to provision or to patch. If an instance is already present then the instance location references will be remapped to current installation.
Apache User	no default	The user under which the Apache server will run under. The user will be created if not present and the password for the newly created user can be set using Apache HTTP User Password parameter.
Httpd Distribution Archive	True	The .zip or tar archive that contains the Apache installed archive.
Apache Installation Location	no default	The installation location for Apache server.
Instance HTTP Port	True	Comma separated list of the HTTP Ports to be used in running the instances. This value must be in correspondence to the instance location.
Staging Location	no default	The temporary location to download the HTTPd distribution package.

Parameters in the step: Gather Advanced Parameters for Apache Provision Software

Parameter Name	Default Value	Description
Apache	no	Comma separated list of absolute path to the content homes. The

Parameters in the step: Gather Advanced Parameters for Apache Provision Software, continued

Parameter Name	Default Value	Description
Content Location	default	values are in correspondence to the instance home location.
Apache HTTP User Password	no default	This is required when the Apache HTTP user does not exist and the user must be created. This will be the password of the newly created user. This is mandatory if the target machine is running Windows OS.
Cleanup Existing Installation	no default	If "True" is specified, the process will be stopped and the location will be erased if the workflow runs successfully. If "False" is specified, the workflow fails when there is a conflict. Valid values are "True" and "False".
Cleanup On Failure	True	Determines whether to remove downloaded and extracted files as well as cleans up installed directory on failure of workflow. Default is set to True, which will clean up on failure.
Cleanup On Success	True	Determines whether to remove downloaded and extracted files as well as cleans up installed directory on successful execution of workflow. Default is set to True, which will clean up on failure.
Enable SSL	False	Enables the Server Side Includes feature for the content directory. The values are 'True' or 'False'.
Instance SSL Port	no default	Comma separated list of values corresponding to an instance name. This will be used to initialize the listener port in the SSL configuration file. Example: If Instance Name Parameter value is http_instance1,http_instance2, the port values can be 1234,4321 where 1234 belongs to http_instance1 and 4321 belongs to http_instance2.
Overwrite Service	False	The values of this parameter can be True or False . If True is specified, then the service which already exists will be backed up and overwritten.
SSL Cert File	no default	Comma separated list of paths to the SSL cert file. This value will be updated in the SSL configuration of instance configuration folder.
SSL Key File	True	Comma separated list of paths to the SSL key file. This value will be updated in the SSL configuration of instance configuration folder.
Service Name	no default	Comma separated set of values. The name for the Apache service in a UNIX machine.
IP-Hostname Configuration	no default	Comma separated list of values in the following format: ipaddress1=hostname1,ipaddress2=hostname2,ipaddress3=hostname3 The number of ipaddress=hostname values must be equal to the number of instances to be provisioned by the workflow.

See ["Parameters for Apache - Provision Software"](#) for detailed descriptions of all input parameters for this workflow, including default values.

3. In the workflow editor, expose any additional parameters that you need. You will specify values for those parameters when you create the deployment.
4. Save the changes to the workflow (click **Save** in the lower right corner).
5. Create a new deployment.
6. On the Parameters tab, specify values for the required parameters listed in step 2 and any additional parameters that you have exposed. You do not need to specify values for those parameters whose default values are appropriate for your environment.
7. On the Targets tab, specify one or more targets for this deployment.
8. Save the changes to the workflow (click **Save** in the lower right corner).
9. Run the workflow using this deployment.

The workflow will complete and report “Success” on the Console if it has run successfully. If an invalid parameter value is specified, an error is logged, and the workflow terminates in the “Failure” state.

Sample Scenarios

This topic shows you how to use various parameters to achieve the following provisioning scenarios in your environment using the Apache - Provision Software workflow.

Specify values for the following parameters to install the Apache web server. The downloaded Apache web server binaries will be removed upon successful or unsuccessful execution of the workflow.

Step Name	Parameter Name	Example Value
Gather Parameters for Provisioning Apache Software	Apache Group	apacheusergroup
	Apache Instances	
	Apache User	apacheuser
	Httpd Distribution Archive	apache2.zip
	Apache Installation Location	/tmp/apache/
	Instance HTTP Port	
	Staging Location	/tmp/temp/
Gather Advanced Parameters for Provisioning Tomcat Software	Apache Content Location	httpd.conf
	Apache HTTP User Password	
	Cleanup Existing Installation	True
	Cleanup On Failure	True
	Cleanup On Success	True
	Enable SSL	False

Step Name	Parameter Name	Example Value
	Instance SSL Port	
	Overwrite Service	False
	SSL Cert File	
	SSL Key File	True
	Service Name	
	IP-Hostname Configuration	127.0.0.1=localhost, 192.168.1.123=local@companydomain.com

Be sure that the default values for all remaining parameters are appropriate for your environment.

Parameters for Apache - Provision Software

The following tables describe the required and optional input parameters for this workflow. Several of these parameters are not initially visible in a deployment. For many parameters, if you do not specify a value for a parameter, a default value is assigned.

Parameters in the step: Gather Parameters for Apache Provision Software

Parameter Name	Default Value	Required	Example Value	Description
Apache Group	no default	required	apacheusergroup	The user-group that the Apache server will run under Example: apachegrp. The group will be created if it is not already present
Apache Instances	no default	required		Comma separated list of absolute path to instance locations to provision or to patch. If an instance is already present then the instance location references will be remapped to current installation.
Apache User	no default	required	apacheuser	The user under which the Apache server will run under. The user will be created if not present and the password for the newly created user can be set using Apache HTTP User Password parameter.
Httpd Distribution Archive	True	required	apache2.zip	The .zip or tar archive that contains the Apache installed archive.
Apache Installation Location	no default	required	/tmp/apache/	The installation location for Apache server.
Instance HTTP Port	True	required		Comma separated list of the HTTP Ports to be used in running the instances. This value must be in correspondence to the instance location.
Staging Location	no default	required	/tmp/temp/	The temporary location to download the HTTPd distribution package.

Parameters in the step: Gather Advanced Parameters for Apache Provision Software

Parameter Name	Default Value	Required	Example Value	Description
Apache Content Location	no default	optional	httpd.conf	Comma separated list of absolute path to the content homes. The values are in correspondence to the instance home location.
Apache HTTP User	no default	optional		This is required when the Apache HTTP user does not exist and the user must be created. This will be the password of the newly created user. This is mandatory if the target machine

Parameters in the step: Gather Advanced Parameters for Apache Provision Software, continued

Parameter Name	Default Value	Required	Example Value	Description
Password				is running Windows OS.
Cleanup Existing Installation	no default	optional	True	If "True" is specified, the process will be stopped and the location will be erased if the workflow runs successfully. If "False" is specified, the workflow fails when there is a conflict. Valid values are "True" and "False".
Cleanup On Failure	True	optional	True	Determines whether to remove downloaded and extracted files as well as cleans up installed directory on failure of workflow. Default is set to True, which will clean up on failure.
Cleanup On Success	True	optional	True	Determines whether to remove downloaded and extracted files as well as cleans up installed directory on successful execution of workflow. Default is set to True, which will clean up on failure.
Enable SSL	False	optional	False	Enables the Server Side Includes feature for the content directory. The values are 'True' or 'False'.
Instance SSL Port	no default	optional		Comma separated list of values corresponding to an instance name. This will be used to initialize the listener port in the SSL configuration file. Example: If Instance Name Parameter value is http_instance1,http_instance2, the port values can be 1234,4321 where 1234 belongs to http_instance1 and 4321 belongs to http_instance2.
Overwrite Service	False	optional	False	The values of this parameter can be True or False . If True is specified, then the service which already exists will be backed up and overwritten.
SSL Cert File	no default	optional		Comma separated list of paths to the SSL cert file. This value will be updated in the SSL configuration of instance configuration folder.
SSL Key File	True	optional	True	Comma separated list of paths to the SSL key file. This value will be updated in the SSL configuration of instance configuration folder.
Service Name	no default	optional		Comma separated set of values. The name for the Apache service in a UNIX machine.
IP-Hostname Configuration	no default	optional		<p>Comma separated list of values in the following format:</p> <p>ipaddress1=hostname1,ipaddress2=hostname2,ipaddress3=hostname3</p> <p>The number of ipaddress=hostname values must be equal to the number of instances to be provisioned by the workflow.</p>

Red Hat JBoss

This section contains the following topics:

Workflow type	Workflow name
Provisioning	"Provision Open Source JBoss 7 StandAlone Mode" on the next page
	"JBoss - Provision Software v3" on page 907
Patching	"JBoss - Patch Software v3" on page 918
	"JBoss - Rollback Patch Software v2" on page 926
Configuring	"JBoss - Create and Configure Data Source v2" on page 886
Release Management	"JBoss - Code Release v2" on page 895

Provision Open Source JBoss 7 StandAlone Mode

Use this workflow to install the open source JBoss Application Server 7 Community version (JBoss AS 7) and start a single, default profile application server.

The workflow performs checks to determine whether the JBoss and Java binaries exist on the target server. If they do not, the workflow downloads them from the software repository.

The workflow also performs validation checks at the operating system level, including file system space checks and Java version level checks.

To use this workflow in your environment, see the following information:

Topic	Information Included
"Prerequisites for this Workflow"	List of prerequisites that must be satisfied before you can run this workflow
"How this Workflow Works"	Information about what the workflow does, including validation checks performed, steps executed, and a high-level process flow
"How to Run this Workflow"	Instructions for running this workflow in your environment
"Sample Scenario"	Examples of typical parameter values for this workflow
"Parameters for Provision Open Source JBoss 7 StandAlone Mode"	List of input parameters for this workflow

The process of deploying and running this workflow is the same for all scenarios, but the parameters required will differ depending on the specific scenario that you are implementing.

The workflow provides default values for most parameters. These default values are usually sufficient for a typical provisioning scenario. You can override the defaults by specifying parameter values in the deployment. You can also expose additional parameters in the workflow, if necessary, to accomplish more advanced scenarios.

Any parameters not explicitly specified in the deployment will have the default values listed in ["Parameters for Provision Open Source JBoss 7 StandAlone Mode" on page 885](#).

Note: For information about the steps in this workflow, see the [Steps in this Workflow](#).

Prerequisites for this Workflow

The following prerequisites must be satisfied before you can run the "[Provision Open Source JBoss 7 StandAlone Mode](#)" workflow:

1. The workflow requires unchallenged `sudo` access to a user (typically root) who can access all required files and directories.
2. The workflow requires the Java Development Kit (JDK) version 1.6 update 24.
3. Adequate disk space must be available to install the JBoss and Java binaries.

For information about prerequisites for JBoss AS 7, refer to the [JBoss Product Documentation](#).

How this Workflow Works

This topic contains the following information about the "[Provision Open Source JBoss 7 StandAlone Mode](#)" workflow:

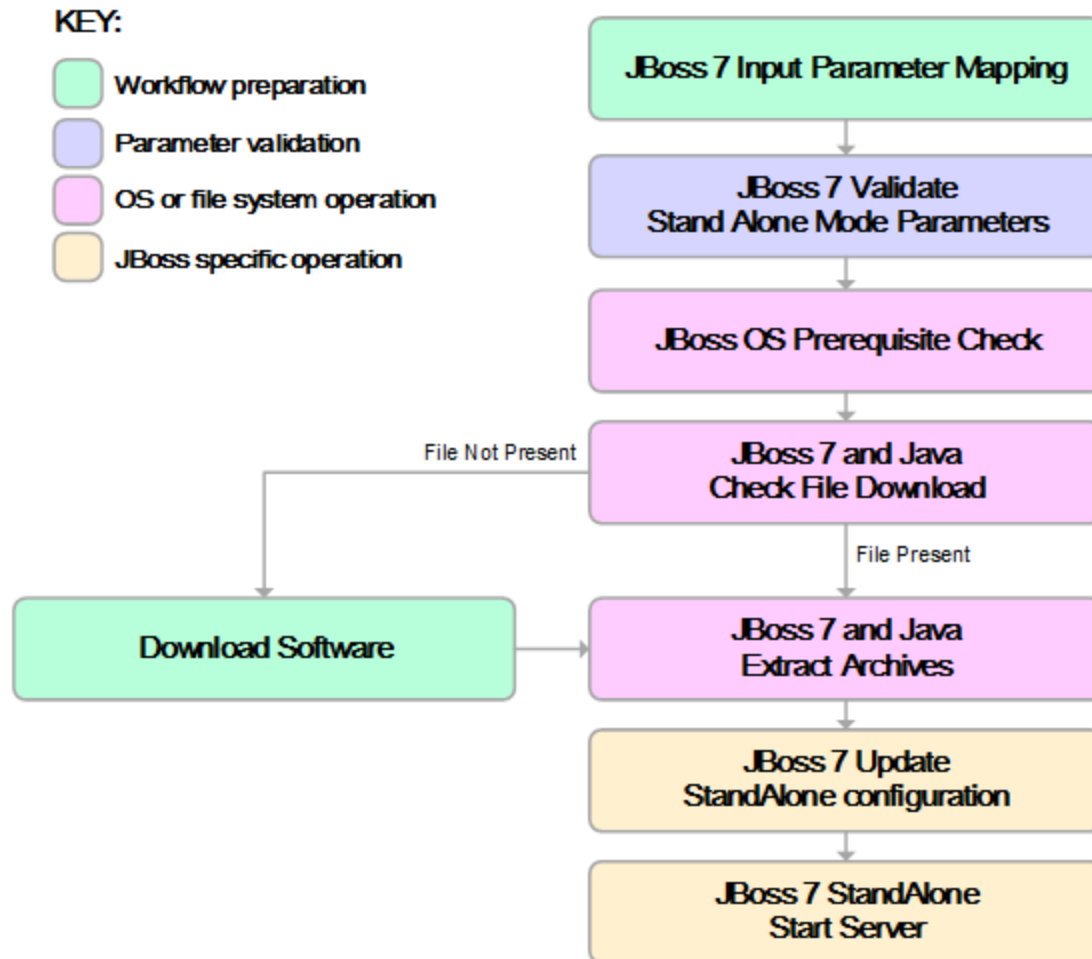
Validation Checks Performed

The workflow checks the following things prior to extracting the binaries. If any of these checks fails, the workflow fails.

1. All required parameters have values. If any required parameter does not have a value—either a value that you specify or a default value—the workflow fails.
2. All required libraries are present (see "[Prerequisites for this Workflow](#)" on the previous page).
3. Sufficient disk space is available to extract the binary files from the compressed archive.
4. Sufficient disk space is available to install JBoss and Java.

Steps Executed

The "Provision Open Source JBoss 7 StandAlone Mode" workflow includes the following steps. Each step must complete successfully before the next step can start. If a step fails, the workflow reports a failure, and all subsequent steps are skipped.



Process Flow

This workflow performs the following tasks:

1. Creates the call wrapper and determines the target server platform type.
2. Validates the parameters needed to install JBoss and Java and create a stand-alone profile (see the [validation checks](#) performed).
3. Checks the following:
 - a. File system space requirements where JBoss and Java will be installed.
 - b. Temporary space requirements where the compressed software will be extracted before it is installed.
4. Determines whether the JBoss and Java binary archives are present on the target server. If either archive is not present, the workflow downloads it from the software repository.
5. Extracts the JBoss and Java binary archives to the specified directories.
6. Creates a default profile for a stand-alone application server.
7. Starts the new stand-alone JBoss application server.
8. Cleans up any files that were downloaded.

How to Run this Workflow

This topic explains how to customize and run the ["Provision Open Source JBoss 7 StandAlone Mode"](#) workflow in your environment.

Note: Prior to running this workflow, review the ["Prerequisites for this Workflow"](#), and ensure that all requirements are satisfied.

To customize and run the Provision Open Source JBoss StandAlone Mode workflow:

1. Create a deployable copy of the workflow
2. Determine the values that you will specify for the following parameter. These are the parameters that are visible in the deployment by default.

Parameter Name	Default Value	Description
Install Dir	UNIX: /opt/jboss Windows: c:\jboss	Fully qualified path where the JBoss and Java binaries will be uncompressed..
JBoss Binary Archive	no default	Fully qualified path where the compressed Java software package should be found on the target server. If the Java software package is not available in this location, it will be downloaded from the SASoftware repository and placed in this location.
Java Binary Archive	no default	Fully qualified path where the compressed Java software package should be found on the target server. If the Java software package is not available in this location, it will be downloaded from the SASoftware repository and placed in this location.
JBoss User	root	The user who will install and run JBoss. This user must have write permission on the install directory.

See ["Parameters for Provision Open Source JBoss 7 StandAlone Mode" on page 885](#) for detailed descriptions of all input parameters for this workflow, including default values.

3. In the workflow editor, expose any additional parameters that you need. You will specify values for those parameters when you create the deployment.
4. Save the changes to the workflow (click **Save** in the lower right corner).
5. Create a new deployment.

6. On the Parameters tab, specify values for the required parameters listed in step 2 and any additional parameters that you have exposed. You do not need to specify values for those parameters whose default values are appropriate for your environment.
7. On the Targets tab, specify one or more targets for this deployment.
8. Save the deployment (click **Save** in the lower right corner).
9. Run the workflow using this deployment.

Sample Scenario

This topic shows you how to use various parameters to achieve the following provisioning scenario in your environment using the ["Provision Open Source JBoss 7 StandAlone Mode"](#) workflow:

Install JBoss Application Server 7 Community version

Specify values for the following parameters to install JBoss AS 7 and start a single, default profile application server. This is the simplest scenario, and it uses only those parameters that are visible in the deployment by default (out of the box).

Step Name	Parameter Name	Example Value
JBoss 7: Validate Stand Alone Mode Parameters	Install Dir	/opt/jboss/jboss-as7
	JBoss Binary Archive	/opt/jboss/jboss-as-7.1.1.Final.zip
	Java Binary Archive	/opt/jboss/jdk-6u29-linux-x64.bin
	JBoss User	root

Be sure that the default values for all remaining parameters are appropriate for your environment (see ["Parameters for Provision Open Source JBoss 7 StandAlone Mode"](#) on the next page).

Parameters for Provision Open Source JBoss 7 StandAlone Mode

The following tables describe the required and optional input parameters for this workflow. Most of these parameters are not initially visible in a deployment. For most parameters, if you do not specify a value for a parameter, a default value is assigned

Parameters Defined in this Step: JBoss 7: Validate Stand Alone Mode Parameters

Parameter Name	Default Value	Required	Description
Call Wrapper	see description	optional	Command that will execute this step (or subsequent steps) as a specific user. For UNIX targets, the default is: <code>/opt/hp/dma/client/jython.sh</code> running as root. For Windows targets, the default is: <code>jython</code> running as Administrator.
File List	no default	optional	Comma-separated list of fully qualified files (JBoss Binary Archive, Java Binary Archive) that must either exist on the target server or be downloaded from the software repository.
HostName	no default	required	Fully qualified hostname or IP address of the server where JBoss will be installed.
Install Dir	UNIX: <code>/opt/jboss</code> Windows: <code>c:\jboss</code>	optional	Fully qualified path where the JBoss and Java binaries will be uncompressed..
JBoss Binary Archive	no default	required	Fully qualified path where the compressed Java software package should be found on the target server. If the Java software package is not available in this location, it will be downloaded from the SAsoftware repository and placed in this location.
JBoss Home	no default	optional	Fully qualified path from which JBoss will run.
JBoss User	root	optional	The user who will install and run JBoss. This user must have write permission on the install directory.
Java Binary Archive	no default	optional	Fully qualified path where the compressed Java software package should be found on the target server. If the Java software package is not available in this location, it will be downloaded from the SAsoftware repository and placed in this location.
Java Home	no default	optional	Fully qualified path from which Java will run.

JBoss - Create and Configure Data Source v2

This workflow creates a data source for a given JBoss Application Server. The data source can be used later by applications deployed to the configured database. The workflow can create a data source for databases on the same machine as well as on remote machines.

To use this workflow in your environment, see the following information:

Topic	Information Included
"Prerequisites for this Workflow"	List of prerequisites that must be satisfied before you can run this workflow
"How this Workflow Works"	Information about what the workflow does, including validation checks performed, steps executed, and a high-level process flow
"How to Run this Workflow"	Instructions for running this workflow in your environment
"Sample Scenarios"	Examples of typical parameter values for this workflow
Parameters	List of input parameters for this workflow

Prerequisites for this Workflow

Be sure that the following prerequisites are satisfied before you run the JBoss - Create and Configure Data Source v2 workflow.

Product Platform

This workflow creates a new JBoss Data Source connection for JBoss EAP 6.x and JBoss WildFly in standalone mode.

Dependencies

The JBoss Application server must be provisioned, up, and running. The database to which the connection is being created must already be installed.

How this Workflow Works

The following information describes how the JBoss - Create and Configure Data Source v2 workflow works:

Overview

This workflow does the following things in the order shown:

1. Initially, the workflow inputs all parameters, set defaults for optional parameters, and validates all parameters.
2. Next the workflow creates and configures the JDBC provider and data source on JBoss Application Server.
3. Finally, the workflow verifies that the connection to the data source was successful.

Validation Checks Performed

The workflow performs the following checks on the input parameters:

Implementation Type	Must be xa or non-xa
JBoss Home Data Source Name Driver Name Connection URL Driver Class Path Implementation Type JNDI Name	Must be specified if Implementation Type is set to non-xa
XA Datasource Class Name XA DataSource Database Name XA DataSource Port XA DataSource Server Name JNDI Name Connection URL JBoss Home Implementation Type Data Source Name	Must be specified if Implementation Type is set to xa
JNDI Name	Must start with java:/ or java:jboss/

The JBoss - Create and Configure Data Source v2 workflow also checks the environment for the following:

- The operating system is supported.
- The JBoss version is EAP 6.x or later.
- The JBoss installation location is valid.
- The driver class path must exist.

Steps Executed

The JBoss - Create and Configure Data Source v2 workflow includes the following steps. Each step must complete successfully before the next step can start. If a step fails, the workflow reports a failure and all subsequent steps are skipped.

Steps Used in the JBoss - Create and Configure Data Source v2 Workflow

Workflow Step	Description
Gather Parameters for JBoss Data Source	This step gathers mandatory input parameters from the user to create a data source on JBoss Application Server standalone setup.
Gather Advanced Parameters for JBoss Data Source	<p>This step prepares and validates the parameters needed to configure a JDBC provider, J2C alias, and data source for a WebSphere Application Server.</p> <p>This step gathers the advanced input parameters to create a data source on a JBoss Application Server. Input parameters specified in this step are optional.</p>
Validate Parameters for JBoss Data Source v2	This step validates the basic and advanced parameters provided by the user, and checks the prerequisites for creating a data source on a JBoss Application Server on standalone setup.
Create JBoss Data Source v3	This step creates and configures the JDBC provider and data source on JBoss Application Server.
Verify Connection for JBoss Data Source v2	This step verifies the connection created by the workflow. If the test connection fails, then the workflow fails as well.

For parameter descriptions and defaults, see ["Parameters for JBoss - Create and Configure Data Source v2" on page 893](#).

How to Run this Workflow

The following instructions show you how to customize and run the JBoss - Create and Configure Data Source v2 workflow in your environment.

The workflow provides default values for some parameters. These default values are usually sufficient for a "typical" installation. You can override the defaults by specifying parameter values in the deployment. You can also expose additional parameters in the workflow, if necessary, to accomplish more advanced scenarios. Any parameters not explicitly specified in the deployment will have the default values listed in ["Parameters for JBoss - Create and Configure Data Source v2" on page 893](#).

Note: Before following this procedure, review the ["Prerequisites for this Workflow" on page 886](#), and ensure that all requirements are satisfied.

To use the JBoss - Create and Configure Data Source v2 workflow:

1. Create a deployable copy of the workflow.
2. Determine the values that you will specify for the following parameters:

Input Parameters for Gather Parameters for JBoss Create and Configure Data Source

Parameter Name	Default Value	Required	Description
Connection URL	no default	required	The URL used by the data source to connect to the database. For example: jdbc:oracle:thin:@//localhost:1521
Data Source Name	no default	required	The name given to the data source when it is created.
Driver Class Path	no default	required	The JAR file name for the resource provider classes. For example: /app/oracle/jdbc/ojdbc6.jar
Driver Name	no default	required	The full path of the driver name. For example: oracle.jdbc.OracleDriver
Driver Type	no default	required	The name of the driver type. For example: 'oracle', 'MS-SQL', etc.
Implementation Type	no default	required	The implementation type for the JDBC (Java Database Connectivity) provider. Use Connection pool data source if your application runs in a single phase or a local transaction. Otherwise, use XA data source to run in a global transaction. Valid values are Connection pool data source or XA data source.
JBoss Home	no default	required	The JBoss installation location.
JNDI Name	no default	required	Java Name Directory Interface (JNDI) name. This is a user specified string specific to the application component calls to the data source. For example: jdbc/myDataSource
Password	no default	required	The database password.
User Name	no default	required	The user name of the database.

Input Parameters for Gather Advanced Parameters for JBoss Create and Configure Data Source

Parameter Name	Default Value	Required	Description
XA DataSource Database Name	no default	optional	If XA is the Implementation Type, then provide the database name.
XA	no	optional	If XA is the Implementation Type, then provide the

Input Parameters for Gather Advanced Parameters for JBoss Create and Configure Data Source, continued

Parameter Name	Default Value	Required	Description
DataSource Port	default		port number.
XA DataSource Server Name	no default	optional	If XA Datasource is provided, then add the fully-qualified Server Name.
XA Datasource Class Name	no default	optional	If XA is the Implementation Type, then provide the Datasource Class. For example: 'com.mysql.jdbc.jdbc2.optional.MysqlXADataSource'

Tip: To avoid having to re-enter passwords whenever they change, you can create a policy to provide them to the workflow.

Note: This is the minimum set of parameters required to run this workflow. You may need to expose additional parameters depending on your objectives.

See ["Parameters for JBoss - Create and Configure Data Source v2" on page 893](#) for detailed descriptions of all input parameters for this workflow, including default values.

2. In the workflow editor, expose any additional parameters that you need. You will specify values for those parameters when you create the deployment.
3. Save the changes to the workflow (click **Save** in the lower right corner).
4. Create a new deployment.
5. On the Parameters tab, specify values for the required parameters listed in step 2 and any additional parameters that you have exposed. You do not need to specify values for those parameters whose default values are appropriate for your environment.
6. On the Targets tab, specify one or more targets for this deployment.
7. Save the deployment (click **Save** in the lower right corner).
8. Run the workflow using this deployment.

Sample Scenarios

This topic shows you typical parameter values for different use cases for the JBoss - Create and Configure Data Source v2 workflow. For a complete list of all parameters used in this workflow,

including default values, see ["Parameters for JBoss - Create and Configure Data Source v2" on page 893](#).

The sample scenarios assume that Web Service URL has the value of DMA.URL. This is the default value mapped from the DMA metadata.

Tip: To avoid having to re-enter passwords whenever they change, you can create a policy to provide them to the workflow.

Scenario 1: Create an Oracle data source using a connection pool data source (non-XA)

In this scenario we will create an Oracle data source using a connection pool data source, where both JBoss and Oracle are installed on same machine.

Input Parameters for Gather Parameters for JBoss Data Source

Parameter Name	Example Value	Description
Connection URL	jdbc:oracle:thin:@localhost:1521/orcl	The URL used by the data source to connect to the database. For example: jdbc:oracle:thin:@//localhost:1521
Data Source Name	myOraclePool	The name given to the data source when it is created.
Driver Class Path	/tmp/jar/ojdbc6.jar	The JAR file name for the resource provider classes. For example: /app/oracle/jdbc/ojdbc6.jar
Driver Name	oracle.jdbc.OracleDriver	The full path of the driver name. For example: oracle.jdbc.OracleDriver
Driver Type	Oracle	The name of the driver type. For example: 'oracle', 'MS-SQL', etc.
Implementation Type	non-xa	The implementation type for the JDBC (Java Database Connectivity) provider. Use Connection pool data source if your application runs in a single phase or a local transaction. Otherwise, use XA data source to run in a global transaction. Valid values are Connection pool data source or XA data source.
JBoss Home	/opt/jboss/wildfly-8.1.0/	The JBoss installation location.
JNDI Name	java:/jboss/MyOracleCpool	Java Name Directory Interface (JNDI) name. This is a user specified string specific to the application component calls to the data source. For example: jdbc/myDataSource

Input Parameters for Gather Parameters for JBoss Data Source, continued

Parameter Name	Example Value	Description
Password	Test	The database password.
User Name	User_test	The user name of the database.

Scenario 2: Create an Oracle data source using a connection pool data source (XA)

In this scenario we will create an Oracle data source using a connection pool data source, where Oracle is installed on a remote machine.

Input Parameters for Gather Parameters for JBoss Data Source

Parameter Name	Example Value	Description
Connection URL	jdbc:oracle:thin:@remoteHost.xyz.com:1521/orcl	The URL used by the data source to connect to the database. For example: jdbc:oracle:thin:@//localhost:1521
Data Source Name	myOraclePool	The name given to the data source when it is created.
Driver Class Path	/tmp/jar/ojdbc6.jar	The JAR file name for the resource provider classes. For example: /app/oracle/jdbc/ojdbc6.jar
Driver Name	oracle.jdbc.OracleDriver	The full path of the driver name. For example: oracle.jdbc.OracleDriver
Driver Type	Oracle	The name of the driver type. For example: 'oracle', 'MS-SQL', etc.
Implementation Type	xa	The implementation type for the JDBC (Java Database Connectivity) provider. Use Connection pool data source if your application runs in a single phase or a local transaction. Otherwise, use XA data source to run in a global transaction. Valid values are Connection pool data source or XA data source.
JBoss Home	/opt/jboss/wildfly-8.1.0/	The JBoss installation location.
JNDI Name	java:/jboss/MyOracleCpool	Java Name Directory Interface (JNDI) name. This is a user specified string specific to the application component calls to the data source. For example: jdbc/myDataSource
Password	Test	The database password.
User Name	User_test	The user name of the database.

Input Parameters for Gather Advanced Parameters for JBoss Data Source

Parameter Name	Example Value	Description
XA DataSource Database Name	remoteHost.xyz.com	If XA is the Implementation Type, then provide the database name.
XA DataSource Port	Orcl	If XA is the Implementation Type, then provide the port number.
XA DataSource Server Name	1521	If XA Datasource is provided, then add the fully-qualified Server Name.
XA Datasource Class Name	oracle.jdbc.xa.client. OracleXADataSource	If XA is the Implementation Type, then provide the Datasource Class. For example: 'com.mysql.jdbc.jdbc2.optional.MysqlXADataSource'

Parameters for JBoss - Create and Configure Data Source v2

The following tables describe the required and optional input parameters for this workflow. Most of these parameters are not initially visible in a deployment. For most parameters, if you do not specify a value for a parameter, a default value is assigned.

Input Parameters for Gather Parameters for JBoss Data Source

Parameter Name	Default Value	Required	Description
Connection URL	no default	required	The URL used by the data source to connect to the database. For example: jdbc:oracle:thin:@//localhost:1521
Data Source Name	no default	required	The name given to the data source when it is created.
Driver Class Path	no default	required	The JAR file name for the resource provider classes. For example: /app/oracle/jdbc/ojdbc6.jar
Driver Name	no default	required	The full path of the driver name. For example: oracle.jdbc.OracleDriver
Driver Type	no	required	The name of the driver type. For example: 'oracle', 'MS-

Input Parameters for Gather Parameters for JBoss Data Source, continued

Parameter Name	Default Value	Required	Description
	default		SQL', etc.
Implementation Type	no default	required	The implementation type for the JDBC (Java Database Connectivity) provider. Use Connection pool data source if your application runs in a single phase or a local transaction. Otherwise, use XA data source to run in a global transaction. Valid values are Connection pool data source or XA data source.
JBoss Home	no default	required	The JBoss installation location.
JNDI Name	no default	required	Java Name Directory Interface (JNDI) name. This is a user specified string specific to the application component calls to the data source. For example: <code>jdbc/myDatasource</code>
Password	no default	required	The database password.
User Name	no default	required	The user name of the database.

Input Parameters for Gather Advanced Parameters for JBoss Data Source

Parameter Name	Default Value	Required	Description
XA DataSource Database Name	no default	optional	If XA is the Implementation Type, then provide the database name.
XA DataSource Port	no default	optional	If XA is the Implementation Type, then provide the port number.
XA DataSource Server Name	no default	optional	If XA Datasource is provided, then add the fully-qualified Server Name.
XA Datasource Class Name	no default	optional	If XA is the Implementation Type, then provide the Datasource Class. For example: 'com.mysql.jdbc.jdbc2.optional.MysqlXADataSource'

Tip: To avoid having to re-enter passwords whenever they change, you can create a policy to provide them to the workflow.

Note: This is the minimum set of parameters required to run this workflow. You may need to expose additional parameters depending on your objectives.

JBoss - Code Release v2

This workflow automates the deployment of applications in a JBoss Application Server. In addition to deployment, this workflow can update the JVM Generic Arguments and JVM System Properties on the Web Server, and also provides install options for the deployment of applications.

Some of the install options are provided as parameters to the workflow, or users can specify install options within a file for each of the applications to be deployed. Note, though, that the value provided for parameters takes higher precedence. This workflow supports the verification of the application deployments by providing the URLs.

For successful application deployments, verifications and a list of the applications are maintained in the History file. In cases of unsuccessful application deployments, the workflow rolls back the deployment and restores the last successfully deployed application (if any).

To use this workflow in your environment, see the following information:

Topic	Information Included
"Prerequisites for this Workflow"	List of prerequisites that must be satisfied before you can run this workflow
"How this Workflow Works"	Information about what the workflow does, including validation checks performed, steps executed, and a high-level process flow
"How to Run this Workflow"	Instructions for running this workflow in your environment
"Sample Scenario"	Examples of typical parameter values for this workflow
Parameters	List of input parameters for this workflow

Prerequisites for this Workflow

Be sure that the following prerequisites are satisfied before you run the JBoss - Code Release v2 workflow.

Product Platform

This workflow deploys an application archive on the Red Hat Enterprise Linux platform only .

Dependencies

This workflow requires the JBoss Application Server to be installed beforehand.

For more information about prerequisites for JBoss - Code Release, refer to the [JBoss Product Documentation](#).

How this Workflow Works

The following information describes how the JBoss - Code Release v2 workflow works:

Overview

This workflow does the following things in the order shown:

1. Initially, the workflow inputs all parameters, set defaults for optional parameters, and validates all parameters. If input files do not exist in the specified locations, they are downloaded from the software repository. The workflow performs a checksum to verify that the archive files should be deployed in the Application Server.
2. Next, the workflow creates the installation options. The workflow updates the JVM settings (if any) and then takes a configuration backup. The workflow deploys the specified Application Archive files in the Application Server.
3. If the application deployment succeeds, the workflow tests the URLs for the web servers and copies the application archives.
4. If the application deployment fails, the workflow rolls back the deployment and restores the last successfully deployed application (if any).
5. Finally, the workflow cleans up downloaded files based on the Cleanup on Success and Cleanup on Failure parameters.

Validation Checks Performed

The workflow performs the following checks on the input parameters:

JBoss Home Application Archive File List MD5 Checksum JBoss Code Release History Location JBoss Staging Location	Required parameters must have values specified
Archive Install Option Force Deploy	If set to True (Yes, Y, or T), Archive Install Option All Server Groups and Archive Install Option Server Groups are not specified
Application Archive File List Md5 Checksum	There must be a checksum for each Application Archive file The Application Archive files must be type .ear or .war and have valid absolute paths Checksums must be valid hexadecimal numbers
JBoss Staging Location JBoss Code Release History Location	Must be valid absolute paths Cannot have the same values

The JBoss - Code Release v2 workflow also checks the environment for the following:

- The operating system is supported.
- The JBoss version is EAP 6.x or later.
- The JBoss installation location is valid.

Steps Executed

The JBoss - Code Release v2 workflow includes the following steps. Each step must complete successfully before the next step can start. If a step fails, the workflow reports a failure and subsequent steps are skipped, except for the Cleanup Downloaded Files step.

Steps Used in the JBoss- Code Release v2 Workflow

Workflow Step	Description
Gather Parameters for JBoss Code Release	This step gathers mandatory input parameters (user-provided) used to deploy a list of application archives in a JBoss Application Server.
Gather Advanced Parameters for JBoss Code Release	This step gathers the advanced input parameters (user-provided) used to deploy an application archive for a JBoss Application Server. Input parameters specified in this step are optional.
Validate Parameters for JBoss Code Release	This step validates the basic and advanced parameters provided by the user, and checks the prerequisites for deploying a list of application archives for a JBoss Application Server.
Check File Download	<p>This step checks for the existence of a file before downloading from the Server Automation software repository.</p> <ul style="list-style-type: none"> • Checks if file is in the expected location. • If the file is not in the expected location, generates a list of files for file download.
Download Software	This step downloads a list of files to a specified location on the target server.
Validate Checksum for Archive File	This step verifies the checksum for the archive files and archive setting file (if any) to ensure that the file has not changed and that the correct archives are deployed in the Application Server.
Create Install Options File for Application Archives	This step creates a setting file that includes the install options for the list of application archive files being deployed by the application server.
Update JVM Settings For JBoss Code Release v2	This step updates the JVM settings for the JBoss Application Server, and also performs a backup of the JBoss server configuration.
Deploy Application Archive for JBoss Code Release	Using the user-provided Application Archive files: This step deploys the list of application archives (.war and .ear) in a JBoss Application Server.
If the application deployment succeeds, the following steps are executed	
Verify URLs of Web Server Applications	This step verifies the checksum for the archive files and archive setting file (if any) to ensure that the file has not changed and that the correct archives are deployed in the Application Server.
Copy Application Archives to History	This step creates a setting file that includes the install options for the list of application archive files being deployed by the application server.
Cleanup Downloaded Files	Using the user-provided Application Archive files: This step deploys the list of application archives (.war and .ear) in a JBoss Application Server.
If the application deployment fails, the following steps are executed	
Rollback JVM Settings for JBoss Code Release v2	This step restores the backup of a JBoss Application server configuration.
Undeploy Application Archive for JBoss	This step uninstalls the list of application archives from a JBoss Application Server.

Steps Used in the JBoss- Code Release v2 Workflow, continued

Workflow Step	Description
Code Release v2	
Deploy Application Archive for JBoss Code Release	Using the backup of the Application Archive files: This step deploys the list of application archives (.war and .ear) in a JBoss Application Server.
Cleanup Downloaded Files	For workflow failure—and if Cleanup on Failure is set to True (default)—this step removes all downloaded files and archives. Dependencies: Run as file/directory owner.

For parameter descriptions and defaults see, ["Parameters for JBoss - Code Release v2" on page 905](#).

How to Run this Workflow

The following instructions show you how to customize and run the JBoss - Code Release v2 workflow in your environment.

The workflow provides default values for some parameters. These default values are usually sufficient for a "typical" installation. You can override the defaults by specifying parameter values in the deployment.

Note: Before following this procedure, review the ["Prerequisites for this Workflow"](#), and ensure that all requirements are satisfied.

Before you run this workflow, you can perform the following optional advance configuration to deploy applications JBoss application servers.

Create a configuration file on the target machine or the SA Server. The file should contain the advanced parameters for all the application servers being deployed. If no configuration file is provided, the target will be defaulted to admin server of the domain. The options that are to be used in this file are listed below.

```
AdderEAR.ear = {
  Runtime Name = adder_app
}
myServletWAR.war = {
  Force Deploy=Yes Runtime Name=myservletAPP Keep Content=True
}
```

List of Options:

- Force Deploy
- All Server Groups
- Runtime Name
- Server Groups
- Disabled
- Keep Content

To use the JBoss - Code Release workflow:

1. Create a deployable copy of the workflow.
2. Determine the values that you will specify for the following parameters:

Parameters Defined in this Step: Gather Parameters for JBoss - Code Release

Parameter Name	Default Value	Required	Description
Application Archive File List	no default	required	Comma-separated list of the Application Archive files to be deployed. Example: xxx.war or yyy.ear
JBoss Code Release History Location	/opt/hp/dma/jboss/history	required	Fully qualified path name of the location where the application archive will be saved (for history purposes) on the target machine. This location cannot be the same as the Code Release Staging Location.
JBoss Home	/opt/jboss	required	The location of the JBoss installation.
JBoss Staging Location	/tmp/jboss/stage	required	The temporary location in which to store the application archive. Note that the workflow will fail if the directory does not exist in the location specified.
MD5 Checksum	no default	required	Comma-separated list of the MD5 Checksum of the Application Archive files to be deployed.

Parameters Defined in this Step: Gather Parameters for JBoss - Code Release , continued

Parameter Name	Default Value	Required	Description
Test URLs	no default	required	Comma-separated list of URLs used to test whether or not the list of applications deployed successfully. Example: http://mytestdb.com, http://yourtest.com

Note: This is the minimum set of parameters required to run this workflow. You may need to expose additional parameters depending on your objectives.

See ["Parameters for JBoss - Code Release v2" on page 905](#) for detailed descriptions of all input parameters for this workflow, including default values.

3. In the workflow editor, expose any additional parameters that you need. You will specify values for those parameters when you create the deployment.
4. Save the changes to the workflow (click **Save** in the lower right corner).
5. Create a new deployment.
6. On the Parameters tab, specify values for the required parameters listed in step 2 and any additional parameters that you have exposed. You do not need to specify values for those parameters whose default values are appropriate for your environment.
7. On the Targets tab, specify one or more targets for this deployment.
8. Save the deployment (click **Save** in the lower right corner).
9. Run the workflow using this deployment.

To verify the results:

The workflow will complete and report SUCCESS on the Console if it has run successfully. If an error occurs during workflow execution, the error is logged, and the workflow terminates in the FAILURE state.

Optional: If you want to further verify the results:

Use the WebSphere administrative console interface to check that the web server is configured.

Sample Scenario

This topic shows you typical parameter values for different use cases for the JBoss - Code Release v2 workflow. For a complete list of all parameters used in this workflow, including default values, see ["Parameters for JBoss - Code Release v2" on page 905](#).

Tip: To avoid having to re-enter passwords whenever they change, you can create a policy to provide them to the workflow.

Scenario 1: Install an application archive (for example stockanalysis.war) on a running JBoss Application Server on a standalone setup.

In this scenario we will deploy the stockanalysis.war file on a running JBoss Application Server. We will install the application using the default installation options. If the application archive files are not present in the Code Release Staging Location, then they will be downloaded from the SA Repository.

Parameters Defined in this Step: Gather Parameters for JBoss - Code Release

Parameter Name	Example Value	Description
Application Archive File List	stockanalysis.war	Comma-separated list of the Application Archive files to be deployed. Example: xxx.war or yyy.ear
JBoss Code Release History Location	/opt/hp/dma/jboss/history	Fully qualified path name of the location where the application archive will be saved (for history purposes) on the target machine. This location cannot be the same as the Code Release Staging Location.
JBoss Staging Location	/tmp/jboss/stage	The temporary location in which to store the application archive. Note that the workflow will fail if the directory does not exist in the location specified.
JBoss Home	/opt/jboss/wildfly-9.0.0.Alpha1/	The location of the JBoss installation.
MD5 Checksum	4477e994e9d457ad2214a3d36b1bb16b	Comma-separated list of the MD5 Checksum of the Application Archive files to be deployed.
Test URLs	http://<server:port>/stockanalysis/<xyx.html>	Comma-separated list of URLs used to test whether or not the list of applications deployed successfully. Example: http://mytestdb.com , http://yourtest.com

Scenario 2: Install an application archive (for example stockanalysis.war) on a running JBoss Application Server on a standalone setup.

In this scenario we will deploy the stockanalysis.war file on a running JBoss Application Server. We will install the application using the default installation options. The JVM settings are also applied to the Application server. If the application archive files are not present in the Code Release Staging Location, then they will be downloaded from the SA Repository.

Parameters Defined in this Step: Gather Parameters for JBoss - Code Release

Parameter Name	Example Value	Description
Application Archive File List	stockanalysis.war	Comma-separated list of the Application Archive files to be deployed. Example: xxx.war or yyy.ear
JBoss Code Release History Location	/opt/hp/dma/jboss/history	Fully qualified path name of the location where the application archive will be saved (for history purposes) on the target machine. This location cannot be the same as the Code Release Staging Location.
JBoss Staging Location	/opt/hp/dma/jboss/history	The temporary location in which to store the application archive. Note that the workflow will fail if the directory does not exist in the location specified.
JBoss Home	/opt/jboss/wildfly-9.0.0.Alpha1/	The location of the JBoss installation.
MD5 Checksum	4477e994e9d457ad2214a3d36b1bb16b	Comma-separated list of the MD5 Checksum of the Application Archive files to be deployed.
Test URLs	http://<server:port>/stockanalysis/<xyx.html>	Comma-separated list of URLs used to test whether or not the list of applications deployed successfully. Example: http://mytestdb.com , http://yourtest.com

Parameters Defined in this Step: Gather Advanced Parameters for JBoss - Code Release

Parameter Name	Example Value	Description
JVM Generic Arguments	<ul style="list-style-type: none"> Dclient.encoding.override=UTF-8 Dsun.rmi.dgc.client.gcInterval=3600000000 Dsun.rmi.dgc.server.gcInterval=3600000000 	Specifies the JVM generic arguments. Provide values as standard JVM settings.

Parameters Defined in this Step: Gather Advanced Parameters for JBoss - Code Release , continued

Parameter Name	Example Value	Description
JVM System Properties	stockanalysis_home, /opt/stockanalysis/bin, Home path for the stock analysis	Specifies the JVM System Properties. Provide the string in the following format: 'PropertyName, PropertyValue PropertyName, PropertyValue'

Parameters for JBoss - Code Release v2

The following tables describe the required and optional input parameters for this workflow. For most parameters, if you do not specify a value for a parameter, a default value is assigned.

Determine the values that you will specify for the following parameters:

Parameters Defined in this Step: Gather Parameters for JBoss - Code Release

Parameter Name	Default Value	Required	Description
Application Archive File List	no default	required	Comma-separated list of the Application Archive files to be deployed. Example: xxx.war or yyy.ear
JBoss Code Release History Location	/opt/hp/dma/jboss/history	required	Fully qualified path name of the location where the application archive will be saved (for history purposes) on the target machine. This location cannot be the same as the Code Release Staging Location.
JBoss Home	/opt/jboss	required	The location of the JBoss installation.
JBoss Staging Location	/tmp/jboss/stage	required	The temporary location in which to store the application archive. Note that the workflow will fail if the directory does not exist in the location specified.
MD5 Checksum	no default	required	Comma-separated list of the MD5 Checksum of the Application Archive files to be deployed.
Test URLs	no default	required	Comma-separated list of URLs used to test whether or not the list of applications deployed successfully. Example: http://mytestdb.com , http://yourtest.com

Parameters Defined in this Step: Gather Advanced Parameters for JBoss - Code Release

Parameter Name	Default Value	Required	Description
Archive Install Option All Server Groups	no default	optional	This parameter specifies whether or not the deployment is applicable to all available server groups. Note: This argument is unavailable in standalone mode.
Archive Install Option Force Deploy	True	optional	This parameter specifies whether or not the existing application is replaced by the new one. A value of True replaces the application, and a value of False ensures that it is not replaced.
Archive Install Option Runtime Name	no default	optional	Specifies the runtime name of the deployment.
Archive Install Option Server Groups	no default	optional	This parameter specifies a comma-separated list of server group names to which the deployment should apply. Note: This argument is unavailable in standalone mode.
Archive Settings File	no default	optional	The file containing the install options for all the archive files.
Cleanup on Failure	True	optional	Determines whether or not to remove downloaded and extracted files. This parameter also cleans up the installed directory upon failure of the workflow.
Cleanup on Success	True	optional	Determines whether or not to remove downloaded and extracted files. This parameter also cleans up the installed directory upon successful execution of the workflow.
JVM Generic Arguments	no default	optional	Specifies the JVM generic arguments. Provide values as standard JVM settings.
JVM System Properties	no default	optional	Specifies the JVM System Properties. Provide the string in the following format: 'PropertyName, PropertyValue PropertyName, PropertyValue'

JBoss - Provision Software v3

Use this workflow to install a new instance of a standalone JBoss Application Server supporting community edition 7.1.1 and 7.2.0, Enterprise Application Platform (EAP), and WildFly versions.

The workflow performs checks to determine whether the JBoss and Java binaries exist on the target server. If they do not, the workflow downloads them from the software repository.

The workflow also performs validation checks at the operating system level, including file system space checks and Java version level checks.

Topic	Information Included
"Prerequisites for this Workflow"	List of prerequisites that must be satisfied before you can run this workflow
"How this Workflow Works"	Information about what the workflow does, including validation checks performed, steps executed, and a high-level process flow
"How to Run this Workflow"	Instructions for running this workflow in your environment
"Sample Scenarios"	Examples of typical parameter values for this workflow
"Parameters for JBoss - Provision Software v3"	List of input parameters for this workflow

The process of deploying and running this workflow is the same for all scenarios, but the parameters required will differ depending on the specific scenario that you are implementing.

The workflow provides default values for most parameters. These default values are usually sufficient for a typical provisioning scenario. You can override the defaults by specifying parameter values in the deployment. You can also expose additional parameters in the workflow, if necessary, to accomplish more advanced scenarios.

Any parameters not explicitly specified in the deployment will have the default values listed in ["Parameters for JBoss - Provision Software v3"](#).

Note: For information about the steps in this workflow, see the [Steps in this Workflow](#).

Note: The documentation for this workflow contains steps that are referred to by their base names. The names in the DMA user interface may have a version appended, for example, v2.

Prerequisites for this Workflow

The following prerequisites must be satisfied before you can run the ["JBoss - Provision Software v3"](#) workflow:

1. The workflow requires unchallenged `sudo` access to a user (typically root) who can access all required files and directories.
2. The workflow requires the Java Development Kit (JDK) version 1.7 (or later).
3. Adequate disk space must be available to install the JBoss and Java binaries.

For information about prerequisites for JBoss, refer to the [Red Hat JBoss Product Documentation](#).

How this Workflow Works

This topic contains the following information about the "JBoss - Provision Software v3" workflow:

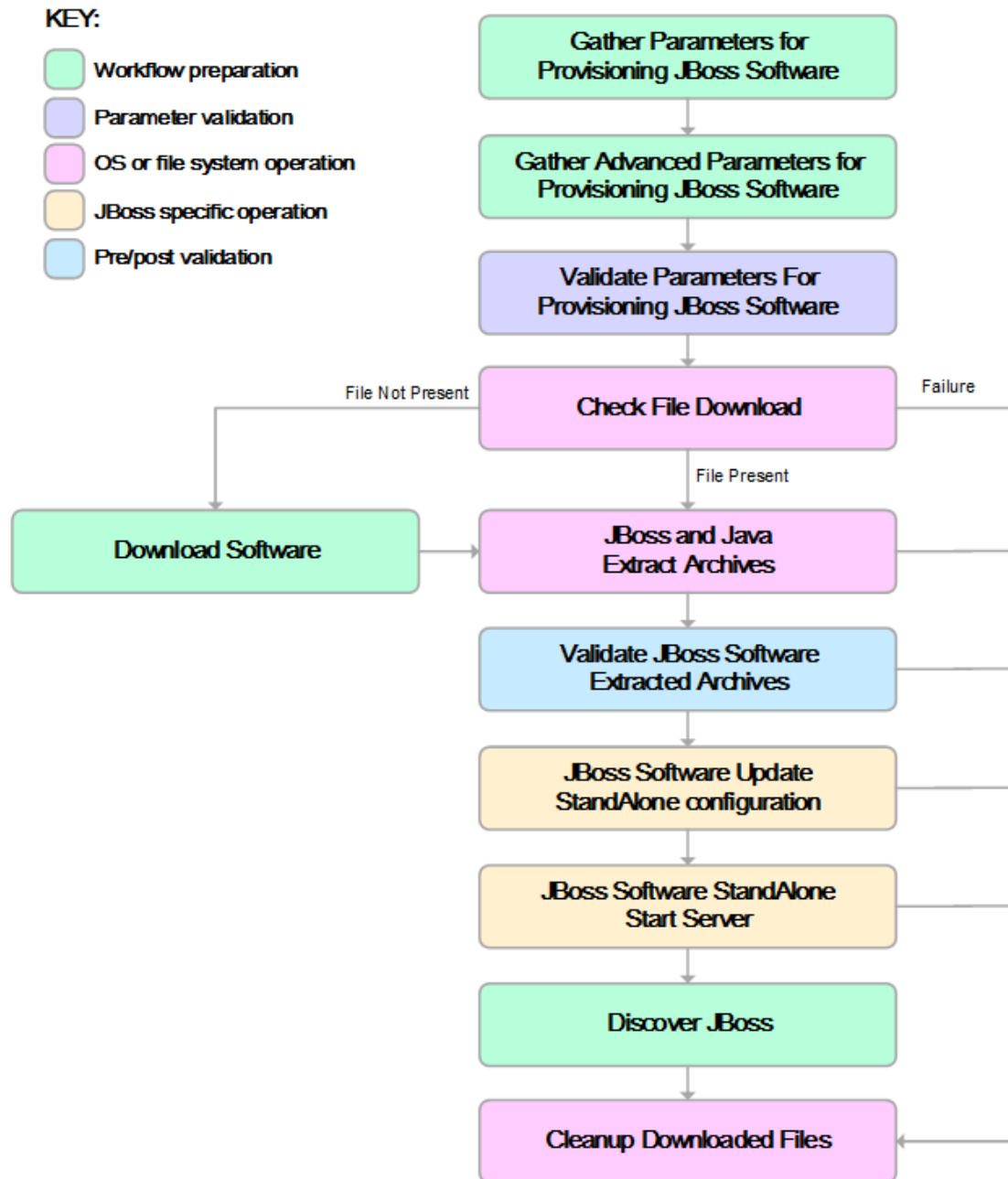
Validation Checks Performed

The workflow checks the following things prior to extracting the binaries. If any of these checks fails, the workflow fails.

1. All required parameters have values. If any required parameter does not have a value—either a value that you specify or a default value—the workflow fails.
2. Directories and host names are valid. No illegal characters are included. The fully qualified paths specified for downloading JBoss and Java binaries exist and point to the same folder, for example: `/example/downloads/`.
3. The Java version is 1.7 or later and the revision is 5 or later.
4. The operating system is a supported platform.
5. Sufficient disk space is available to extract the binary files from the compressed archive.
6. Sufficient disk space is available to install JBoss and Java.

Steps Executed

The "JBoss - Provision Software v3" workflow includes the following steps. Each step must complete successfully before the next step can start. If a step fails, the workflow reports a failure, and subsequent steps are skipped.



Process Flow

This workflow performs the following tasks:

1. Creates the call wrapper and determines the target server platform type.
2. Inputs the required and optional parameters for the workflow.
3. Validates the parameters needed to install JBoss and Java in standalone mode.
4. Determines whether the JBoss and Java binary archives are present on the target server. If either archive is not present, the workflow downloads it from the software repository.
5. Extracts the JBoss and Java binary archives to the specified directories.
6. Validates that the Java version is 1.7 or later.
7. Updates the `standalone.xml` configuration file—required to start the server in standalone mode.
8. Starts the new standalone JBoss application server.
9. Captures information learned during the provisioning process in DMA metadata fields.
10. Cleans up downloaded files that are no longer required, based on user-specified flags in the event of workflow success or failure.

How to Run this Workflow

This topic explains how to customize and run the ["JBoss - Provision Software v3"](#) workflow in your environment.

Note: Prior to running this workflow, review the ["Prerequisites for this Workflow"](#), and ensure that all requirements are satisfied.

To customize and run the JBoss - Provision Software workflow:

1. Create a deployable copy of the workflow.
2. Determine the values that you will specify for the following parameters. These are the parameters that are visible in the deployment by default.

Parameter Name	Default Value	Description
Java Binary Archive	no default	Fully qualified path to where the compressed Java software package should be located on the target machine. The directory should exist on the target machine and must be the same directory specified in the JBoss Binary Archive parameter. If the Java software package is not available in this directory, then it will be downloaded from the software repository and placed in this directory. For example: <code>/example/downloads/jdk-7u71-linux-x64.gz</code>
Install Dir	<code>/opt/jboss</code>	Fully qualified path to where the binary files will be uncompressed. For example: <code>/opt/jboss</code>
JBoss Binary Archive	no default	Fully qualified path to where the compressed JBoss software package should be located on the target machine. The directory should exist on the target machine and must be the same directory that is provided in the Java Binary Archive Parameter. If the JBoss software package is not available in this directory, then it will be downloaded from the software repository and placed in this directory. For example: <code>/example/downloads/wildfly-9.0.0.Alpha1.tar.gz</code>
Download Location	no default	The location where the Java and JBoss binaries will be downloaded and saved in the target machine.
Web Service Password	no default	Password for the DMA Discovery web service API.
Web Service URL	no default	URL for the DMA Discovery web service API.
Web Service User	no default	User capable of modifying the managed environment through the DMA Discovery web service API.

See "[Parameters for JBoss - Provision Software v3](#)" for detailed descriptions of all input parameters for this workflow, including default values.

3. In the workflow editor, expose any additional parameters that you need. You will specify values for those parameters when you create the deployment.
4. Save the changes to the workflow (click **Save** in the lower right corner).
5. Create a new deployment.
6. On the Parameters tab, specify values for the required parameters listed in step 2 and any additional parameters that you have exposed. You do not need to specify values for those parameters whose default values are appropriate for your environment.
7. On the Targets tab, specify one or more targets for this deployment.
8. Save the changes to the workflow (click **Save** in the lower right corner).
9. Run the workflow using this deployment.

The workflow will complete and report "Success" on the Console if it has run successfully. If an invalid parameter value is specified, an error is logged, and the workflow terminates in the "Failure" state.

Sample Scenarios

This topic shows you how to use various parameters to achieve the following provisioning scenarios in your environment using the "JBoss - Provision Software v3" workflow:

Scenario 1: Install JBoss Enterprise Application Platform 6 (EAP)

Specify values for the following parameters to install the EAP 6.3.0 version of JBoss. The downloaded JBoss and Java binaries will be removed upon successful or unsuccessful execution of the workflow.

Step Name	Parameter Name	Example Value
Gather Parameters for Provisioning JBoss Software v2	Install Dir	/opt/jboss
	Download Location	/opt/downloads
	Java Binary Archive	/example/downloads/jdk-7u71-linux-x64.gz
	JBoss Binary Archive	/example/downloads/jboss-eap-6.3.0.zip
	Web Service Password	mypwd
	Web Service URL	https://mydmaservername:8443/dma
Gather Advanced Parameters for Provisioning JBoss Software	Web Service User	myusername
	Clean on Failure	True
	Clean on Success	True
	Install Dir	/opt/jboss

Be sure that the default values for all remaining parameters (the advanced parameters) are appropriate for your environment.

Scenario 2: Install JBoss WildFly

Specify values for the following parameters to install the WildFly 9.0.0 Alpha1 version of JBoss in the `/opt/wildfly` folder. The downloaded JBoss and Java binaries will not be removed upon successful or unsuccessful execution of the workflow. You need to expose the advanced parameters in your copy of the workflow in order to implement this scenario.

Step Name	Parameter Name	Example Value
Gather Parameters for Provisioning JBoss Software v2	Install Dir	<code>/opt/jboss</code>
	Download Location	<code>/opt/downloads</code>
	Java Binary Archive	<code>/example/downloads/jdk-7u71-linux-x64.gz</code>
	JBoss Binary Archive	<code>/example/downloads/wildfly-9.0.0.Alpha1.tar.gz</code>
	Web Service Password	<code>mypwd</code>
	Web Service URL	<code>https://mydmaservername:8443/dma</code>
	Web Service User	<code>myusername</code>
Gather Advanced Parameters for Provisioning JBoss Software	Clean on Failure	<code>True</code>
	Clean on Success	<code>True</code>
	Install Dir	<code>/opt/jboss</code>

Parameters for JBoss - Provision Software v3

The following tables describe the required and optional input parameters for this workflow. Several of these parameters are not initially visible in a deployment. For many parameters, if you do not specify a value for a parameter, a default value is assigned.

Parameters Defined in this Step: Gather Parameters for Provisioning JBoss Software

Parameter Name	Default Value	Required	Description
Install Dir	/opt/jboss	required	Fully qualified path to where the binary files will be uncompressed.
Download Location	no default	required	The location where the Java and JBoss binaries will be downloaded and saved in the target machine.
Java Binary Archive	no default	required	Fully qualified path to where the compressed Java software package should be located on the target machine. The directory should exist on the target machine and must be the same directory specified in the JBoss Binary Archive parameter. If the Java software package is not available in this directory, then it will be downloaded from the software repository and placed in this directory. For example: /example/downloads/jdk-7u71-linux-x64.gz
JBoss Binary Archive	no default	required	Fully qualified path to where the compressed JBoss software package should be located on the target machine. The directory should exist on the target machine and must be the same directory that is provided in the Java Binary Archive Parameter. If the JBoss software package is not available in this directory, then it will be downloaded from the software repository and placed in this directory. For example: /example/downloads/wildfly-9.0.0.Alpha1.tar.gz
Web Service Password	no default	required	Password for the DMA Discovery web service API.
Web Service URL	no default	required	URL for the DMA Discovery web service API.
Web Service User	no default	required	User capable of modifying the managed environment through the DMA Discovery web service API.

Parameters Defined in this Step: Gather Advanced Parameters for Provisioning JBoss Software

Parameter Name	Default Value	Required	Description
Clean on Failure	True	optional	Flag that determines whether to clean up on workflow failure. If set to 'True', the workflow will clean up the downloaded files. Valid values are 'True' and 'False'. The default value is

Parameters Defined in this Step: Gather Advanced Parameters for Provisioning JBoss Software , continued

Parameter Name	Default Value	Required	Description
			'True'.
Clean on Success	True	optional	Flag that determines whether to clean up on workflow success. If set to 'True', the workflow will clean up the downloaded files. Valid values are 'True' and 'False'. The default value is 'True'.
JBoss Group	no default	optional	Group ID to install JBoss software. If not specified, group ID of the root will be used.
JBoss User	no default	optional	The user installing the JBoss. If not specified, root user ID will be used.

JBoss - Patch Software v3

This workflow applies one or more patches to the specified JBoss EAP standalone server and WildFly application server. It also supports patching the Java that is used by WebLogic domains.

To use this workflow in your environment, see the following information:

Topic	Information Included
"Prerequisites for this Workflow"	List of prerequisites that must be satisfied before you can run this workflow
"How this Workflow Works"	Information about what the workflow does, including validation checks performed, steps executed, and a high-level process flow
"How to Run this Workflow"	Instructions for running this workflow in your environment
"Sample Scenario"	Examples of typical parameter values for this workflow
"Parameters for JBoss - Patch Software v3"	List of input parameters for this workflow

Prerequisites for this Workflow

The following prerequisites must be satisfied before you can run the JBoss patching workflow:

- The latest DMA solution packs require the latest DMA platform. To use the latest solution packs, update the DMA platform. DMA10.50.001.000 solution packs are supported on DMA10.50.001.000 (and later).
- You have installed JBoss.
- You have provisioned a JBoss or WildFly server. You can do this by running workflows found in the DMA Application Server Provisioning Solution Pack:
 - Provision JBoss standalone EAP server.
- You have verified that the patches to be installed are appropriate for your version of JBoss or WildFly.
- You have added a link to the Java folder and added the link in the **setDomain.sh** file.

For more information about prerequisites for JBoss or WildFly, refer to the [JBoss Product Documentation](#).

How this Workflow Works

The following information describes how the JBoss - Patch Software V3 workflow works:

Overview

The JBoss - Patch Software workflow first prepares to apply the patch. It creates the commands that will be used to execute subsequent steps, gathers and validates the necessary input parameters, and creates additional utility parameters.

The workflow then makes sure that all necessary files exist, have valid specifications, and are in the expected locations.

Next, the workflow applies the patches. On the Console page, the workflow reports whether each patch succeeded or failed. It collects the patch identifiers of the patches that were successfully installed.

The workflow ends cleanly. It returns all JBoss components to the state they were in when the workflow started. If required, it restarts the JBoss (EAP) standalone server.

This workflow also supports patching the Java that is used by WebLogic domains. A symbolic link to the Java parent directory must be provided and specified in the setDomain.sh file. The Java binaries will be extracted in this folder.

Steps Executed

The JBoss - Patch Software workflow includes the following steps. Each step must complete successfully before the next step can start. If a step fails, the workflow reports a failure and all subsequent steps are skipped.

Workflow Steps

Steps Used in JBoss - Patch Software

Workflow Step	Description
Gather Parameters for Patching JBoss Software	This step gathers mandatory input parameters (user-provided) used to apply a list of patches for JBoss (EAP) Standalone Server.
Gather Advanced Parameters for Patching JBoss Software v2	This step gathers the advanced input parameters (user-provided) used to deploy a patch for JBoss (EAP) Standalone Server. Input parameters specified in this step are optional. Appropriate default values are specified.
Validate Parameters for Patching JBoss Software v3	This step validates the basic and advanced parameters provided by the user, and checks the prerequisites for patching JBoss (EAP) Standalone Server.
Check File Download	<p>This step checks for the existence of a file on the target server before downloading that file from the software repository. For each file in the list, this step does the following things:</p> <ol style="list-style-type: none"> 1. Determines whether the file is in the expected location on the target machine. 2. If the file is not in the expected location, adds that file to a list of files that need to be downloaded.
Decompress Wildfly Patch Archive	This step decompresses WildFly patch archive file to a specified staging location.
Download Software	This step downloads a list of files to a specified location on the target server.
Apply Patch for JBoss Software v2	This step applies the patches to JBoss(EAP) Application Server.
Cleanup Downloaded Files v2	This step removes all temporary downloaded files and archives.
Apply Patch for JBoss Java Home	This Step Extracts the Java JDK or JRE file into the Java home of the JBoss installation.
Cleanup Downloaded Files v2	This step removes all temporary downloaded files and archives.
Restore JBoss Java Home	This step restores the Java Home of the JBoss installation if the Java patching fails.
Discover JBoss	This step examines the target server's physical environment to discover information about JBoss or WildFly.

For parameter descriptions and defaults, see ["Parameters for JBoss - Patch Software v3"](#).

How to Run this Workflow

The following instructions show you how to customize and run the JBoss - Patch Software V3 workflow in your environment.

The workflow provides default values for some parameters. These default values are usually sufficient for a "typical" installation. You can override the defaults by specifying parameter values in the deployment. Any parameters not explicitly specified in the deployment will have the default values listed in "[Parameters for JBoss - Patch Software v3](#)".

Note: Before following this procedure, review the "[Prerequisites for this Workflow](#)", and ensure that all requirements are satisfied.

To use the JBoss - Patch Software workflow:

1. Create a deployable copy of the workflow.
2. Determine the values that you will specify for the following parameters:

Input Parameters for Gather Parameters for Patching JBoss Software

Parameter Name	Default Value	Required	Description
JBoss Home	no default	required	Fully qualified path to the product installation directory in which to install JBoss patches. Example: <code>/opt/jboss/jboss-as-7.0.1.Final/</code>
JBoss Patch Binary Archives	no default	required	Fully qualified path to the comma-separated list of JBoss patch files.
Patch Staging Location	no default	required	The temporary location in which to store the patch archive. Note that the workflow fails if the directory does not exist in the location specified.

Input Parameters for Gather Advanced Parameters for Patching JBoss Software v2

Parameter Name	Default Value	Required	Description
Clean on Failure	True	optional	Determines whether or not to remove downloaded and extracted files. This parameter also cleans up the installed directory upon failure of the workflow.
Clean on Success	True	optional	Determines whether or not to remove downloaded and extracted files. This parameter also cleans up the installed directory upon successful execution of the workflow.
Java JDK File	no default	optional	Name of the Java JDK File. If not present on the target will be downloaded to staging location from SA, for example, <code>jdk-7u80-linux-x64.tar.gz</code> .

Input Parameters for Gather Advanced Parameters for Patching JBoss Software v2, continued

Parameter Name	Default Value	Required	Description
Java JRE File	no default	optional	Name of the Java JRE File. If not present on the target will be downloaded to staging location from SA, for example, jre-7u80-linux-x64.tar.gz.

Note: This is the minimum set of parameters required to run this workflow. You may need to expose additional parameters depending on your objectives.

See "[Parameters for JBoss - Patch Software v3](#)" for detailed descriptions of all input parameters for this workflow, including default values.

3. Save the changes to the workflow (click **Save** in the lower right corner).
4. Create a new deployment.
5. On the Parameters tab, specify values for the required parameters listed in step 2. You do not need to specify values for those parameters whose default values are appropriate for your environment.
6. On the Targets tab, specify one or more targets for this deployment.

Note: Specify all the targets associated with your JBoss (EAP) standalone server. The first target specified must be the Administration Server.

7. Save the deployment (click **Save** in the lower right corner).
8. Run the workflow using this deployment.

To verify the results:

The workflow will complete and report SUCCESS on the Console if it has run successfully. If an error occurs during workflow execution, the error is logged, and the workflow terminates in the FAILURE state.

See the Console page output for error messages that indicate whether problems occurred during the application of the patches. Specifically, look at the JBoss Patch Server step to see the results of applying each individual patch.

Sample Scenario

It is very straightforward to run the JBoss - Patch Software workflow. This topic shows you typical parameter values to use.

Input Parameters for Gather Parameters for Patching JBoss Software

Parameter Name	Example Value	Description
JBoss Home	see description	Fully qualified path to the product installation directory in which to install JBoss patches. Example: /opt/jboss/jboss-eap-6.3
JBoss Patch Binary Archive	see description	Fully qualified path to the comma-separated list of JBoss patch files. Example: /root/jboss-eap-6.3.1-patch.zip,/root/jboss-eap-6.3.2-patch.zip
Patch Staging Location	see description	The temporary location in which to store the patch archive. Note that the workflow fails if the directory does not exist in the location specified. Example: /root

Input Parameters for Gather Advanced Parameters for Patching JBoss Software v2

Parameter Name	Default Value	Required	Description
Clean on Failure	True	optional	Determines whether or not to remove downloaded and extracted files. This parameter also cleans up the installed directory upon failure of the workflow.
Clean on Success	True	optional	Determines whether or not to remove downloaded and extracted files. This parameter also cleans up the installed directory upon successful execution of the workflow.
Java JDK File	no default	optional	Name of the Java JDK File. If not present on the target will be downloaded to staging location from SA, for example, jdk-7u80-linux-x64.tar.gz.
Java JRE File	no default	optional	Name of the Java JRE File. If not present on the target will be downloaded to staging location from SA, for example, jre-7u80-linux-x64.tar.gz.

Parameters for JBoss - Patch Software v3

The following tables describe the required and optional input parameters for this workflow.

Parameters Defined in this Step: Gather Parameters for Patching JBoss Software

Parameter Name	Default Value	Required	Description
JBoss Home	no default	required	Fully qualified path to the product installation directory in which to install JBoss or WildFly patches. Example: /opt/jboss/jboss-as-7.0.1.Final/
JBoss Patch Binary Archive	no default	required	Fully qualified path to the comma-separated list of JBoss patch files. For WildFLy, only one patch binary archive is allowed.
Patch Staging Location	no default	required	The temporary location in which to store the patch archive. Note that the workflow fails if the directory does not exist in the location specified.

Input Parameters for Gather Advanced Parameters for Patching JBoss Software v2

Parameter Name	Default Value	Required	Description
Clean on Failure	True	optional	Determines whether or not to remove downloaded and extracted files. This parameter also cleans up the installed directory upon failure of the workflow.
Clean on Success	True	optional	Determines whether or not to remove downloaded and extracted files. This parameter also cleans up the installed directory upon successful execution of the workflow.
Java JDK File	no default	optional	Name of the Java JDK File. If not present on the target will be downloaded to staging location from SA, for example, jdk-7u80-linux-x64.tar.gz.
Java JRE File	no default	optional	Name of the Java JRE File. If not present on the target will be downloaded to staging location from SA, for example, jre-7u80-linux-x64.tar.gz.

JBoss - Rollback Patch Software v2

This workflow rolls back one or more patches from the specified JBoss or WildFLy application server.

To use this workflow in your environment, see the following information:

Topic	Information Included
"Prerequisites for this Workflow"	List of prerequisites that must be satisfied before you can run this workflow
"How this Workflow Works"	Information about what the workflow does, including validation checks performed, steps executed, and a high-level process flow
"How to Run this Workflow"	Instructions for running this workflow in your environment
" Sample Scenario"	Examples of typical parameter values for this workflow
"Parameters for JBoss - Rollback Patch Software v2"	List of input parameters for this workflow

Prerequisites for this Workflow

The following prerequisites must be satisfied before you can run the JBoss or WildFly rollback patching workflow:

- This solution requires DMA version 10.50 (or later).

The latest DMA solution packs require the latest DMA platform. To use the latest solution packs, update the DMA platform. DMA10.50.001.000 solution packs are supported on DMA10.50.001.000 (and later).

- You have installed JBoss.
- You have provisioned a JBoss EAP server or WildFly application server. You can do this by running workflows found in the DMA Application Server Provisioning Solution Pack:
 - Provision JBoss standalone EAP server.
- You have verified that one or more patches are installed are applied to JBoss or WildFly application server.

For more information about prerequisites for JBoss or WildFly rollback patch, refer to the [JBoss Product Documentation](#).

How this Workflow Works

The following information describes how the JBoss - Rollback Patch Software v2 workflow works:

Overview

The JBoss - Rollback Patch Software workflow first prepares to roll back the patch. It creates the commands that will be used to execute subsequent steps, gathers and validates the necessary input parameters, and creates additional utility parameters.

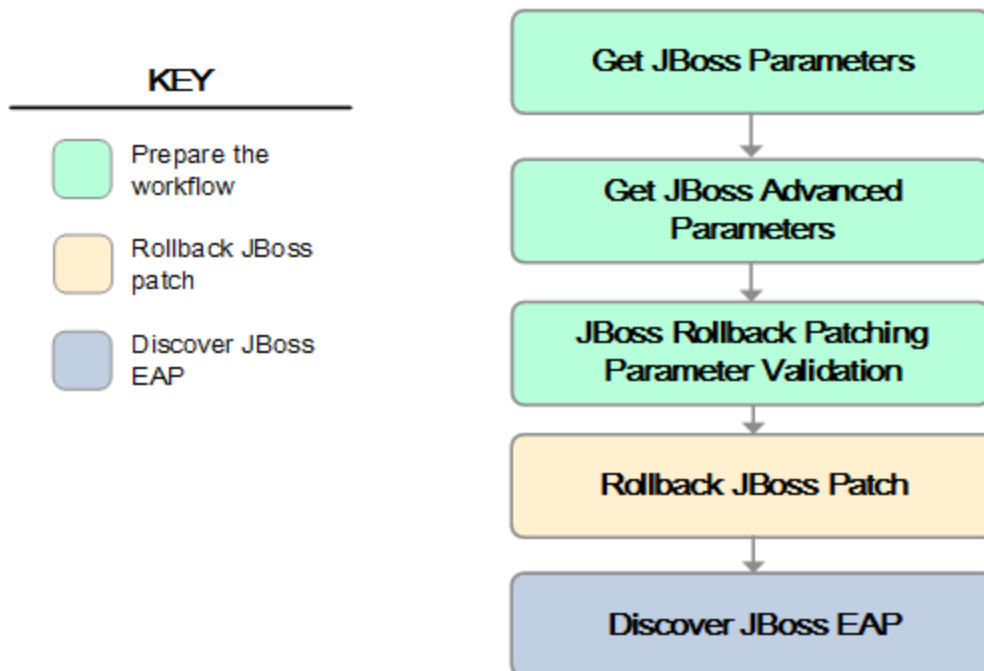
The workflow then makes sure that all necessary files exist, have valid specifications, and are in the expected locations.

Next, the workflow rolls back the patch. On the Console page, the workflow reports if the patch roll back succeeded or failed. It collects the patch identifiers of the patches that were successfully removed.

The workflow ends cleanly. It returns all JBoss or WildFly components to the state they were in when the workflow started. If required, it restarts the JBoss or WildFly application server.

Steps Executed

The JBoss - Rollback Patch Software workflow includes the following steps. Each step must complete successfully before the next step can start. If a step fails, the workflow reports a failure and all subsequent steps are skipped.



Steps Used in JBoss - Rollback Patch Software v2

Workflow Step	Description
Gather Parameters for Rollback Patching JBoss Software	This step gathers mandatory input parameters (user-provided) used to apply a list of patches for JBoss (EAP) Standalone Server or WildFly application server.
Gather Advanced Parameters for Rollback Patching JBoss Software	This step gathers the advanced input parameters (user-provided) used to deploy a patch for JBoss or WildFly application server. Input parameters specified in this step are optional. Appropriate default values are specified.
Validate Parameters for Rollback Patching JBoss Software	This step gathers and validates the parameters required to remove patches from a JBoss or WildFly application server.
Rollback Patch for JBoss Software v2	The step rolls back patches from the specified target.
Discover JBoss	This step examines the target server's physical environment to discover information about JBoss or WildFly.

For parameter descriptions and defaults, see ["Parameters for JBoss - Rollback Patch Software v2" on page 933](#).

How to Run this Workflow

The following instructions show you how to customize and run the JBoss - Rollback Patch Software workflow in your environment.

The workflow provides default values for some parameters. These default values are usually sufficient for a "typical" installation. You can override the defaults by specifying parameter values in the deployment. Any parameters not explicitly specified in the deployment will have the default values listed in ["Parameters for JBoss - Rollback Patch Software v2"](#).

Note: Before following this procedure, review the ["Prerequisites for this Workflow"](#), and ensure that all requirements are satisfied.

To use the JBoss - Rollback Patch Software

1. Create a deployable copy of the workflow.
2. Determine the values that you will specify for the following parameters:

Input Parameters for Gather JBoss Parameters

Parameter Name	Default Value	Required	Description
JBoss Home	no default	required	Fully qualified path to the product installation directory from which to roll back JBoss patches. Example: <code>/opt/jboss/jboss-as-7.0.1.Final/</code>
JBoss Patch IDs	no default	required	Fully qualified path to the comma-separated list of JBoss patch IDs.

Input Parameters for Gather JBoss Advanced Parameters

Parameter Name	Default Value	Required	Description
Override all	True	optional	Bypasses any content verification on the miscellaneous items changed by the patch that is rolled back.
Reset Configuration	True	optional	Updates the installation configuration and resets the snapshots that were taken when the patch was applied.

Note: This is the minimum set of parameters required to run this workflow. You may need to expose additional parameters depending on your objectives.

See ["Parameters for JBoss - Rollback Patch Software v2"](#) for detailed descriptions of all input parameters for this workflow, including default values.

3. In the workflow editor, expose any additional parameters that you need. You will specify values for those parameters when you create the deployment.

4. Save the changes to the workflow (click **Save** in the lower right corner).
5. Create a new deployment.
6. On the Parameters tab, specify values for the required parameters listed in step 2. You do not need to specify values for those parameters whose default values are appropriate for your environment.
7. On the Targets tab, specify one or more targets for this deployment.

Note: Specify all the targets associated with your JBoss (EAP) standalone server. The first target specified must be the Administration Server.

8. Save the deployment (click **Save** in the lower right corner).
9. Run the workflow using this deployment.

To verify the results:

The workflow will complete and report SUCCESS on the Console if it has run successfully. If an error occurs during workflow execution, the error is logged, and the workflow terminates in the FAILURE state.

See the Console page output for error messages that indicate whether problems occurred during the application of the patches. Specifically, look at the JBoss Patch Server step to see the results of applying each individual patch.

Sample Scenario

It is very straightforward to run the JBoss - Rollback Patch Software v2 workflow. This topic shows you typical parameter values to use.

Input Parameters for Gather Parameters for Rollback Patching JBoss Software

Parameter Name	Example Value	Description
JBoss Home	see description	Fully qualified path to the product installation directory from which to roll back JBoss patches. Example: /opt/jboss/jboss-eap-6.3
JBoss Patch IDs	see description	Fully qualified path to the comma-separated list of JBoss patch IDs. Example: jboss-eap-6.3.1.CP

Input Parameters for Gather Advanced Parameters for Rollback Patching JBoss Software

Parameter Name	Example Value	Description
Reset Configuration	see description	Updates the installation configuration and resets the snapshots that were taken when the patch was applied. Valid values are True and False. The default value is True.

Parameters for JBoss - Rollback Patch Software v2

The following tables describe the required and optional input parameters for this workflow.

Parameters Defined in this Step: Gather Parameters for Rollback Patching JBoss Software

Parameter Name	Default Value	Required	Description
JBoss Home	no default	required	Fully qualified path to the product installation directory from which to roll back JBoss patches. Example: /opt/jboss/jboss-as-7.0.1.Final/
JBoss Patch IDs	no default	required	Fully qualified path to the comma-separated list of JBoss patch IDs.

Additional Parameters Defined in this Step: Gather Advanced Parameters for Rollback Patching JBoss Software

Parameter Name	Default Value	Required	Description
Override all	True	optional	If true, this bypasses any content verification on the miscellaneous items changed by the patch that is rolled back.
Reset Configuration	True	optional	If True, this updates the installation configuration and resets the snapshots that were taken when the patch was applied.

Tomcat Application Server

This section contains the following topics:

Workflow type	Workflow name
Provisioning	"Tomcat - Provision Software" on the next page

Tomcat - Provision Software

This workflow deploys an Apache Tomcat Server binary to a specified location and provision multiple Tomcat instances supporting domain configuration. The domain configuration provides the ability to have a Tomcat (Catalina) home folder and multiple instance folders (Catalina base).

For example:

- Catalina Home: /opt/tomcat/apache-tomcat-8.0.1
- Catalina Base1:/vat/tomcat/tomcatinstance-1
- Catalina Base2:/vat/tomcat/tomcatinstance-2

This workflow requires Tomcat version 7.x and 8.x and JDK 1.7 and higher.

Use this workflow to install a new instance of a Apache Tomcat Server version 8.x.

The workflow performs checks to determine whether the Apache Tomcat and Java binaries exist on the target server. If they do not, the workflow downloads them from the software repository.

The workflow also performs validation checks at the operating system level, including file system space checks and Java version level checks.

Topic	Information Included
"Prerequisites for this Workflow"	List of prerequisites that must be satisfied before you can run this workflow
"How this Workflow Works"	Information about what the workflow does, including validation checks performed, steps executed, and a high-level process flow
"How to Run this Workflow"	Instructions for running this workflow in your environment
"Sample Scenarios"	Examples of typical parameter values for this workflow
"Parameters for Tomcat - Provision Software"	List of input parameters for this workflow

The process of deploying and running this workflow is the same for all scenarios, but the parameters required will differ depending on the specific scenario that you are implementing.

The workflow provides default values for most parameters. These default values are usually sufficient for a typical provisioning scenario. You can override the defaults by specifying parameter values in the deployment. You can also expose additional parameters in the workflow, if necessary, to accomplish more advanced scenarios.

Any parameters not explicitly specified in the deployment will have the default values listed in ["Parameters for Tomcat - Provision Software"](#).

Note: For information about the steps in this workflow, see the ["How this Workflow Works"](#) on [page 938](#).

Note: The documentation for this workflow contains steps that are referred to by their base names. The names in the DMA user interface may have a version appended, for example, v2.

Prerequisites for this Workflow

The following prerequisites must be satisfied before you can run the Tomcat - Provision Software workflow:

1. The workflow requires unchallenged `sudo` access to a user (typically root) who can access all required files and directories.
2. The workflow requires the Java Development Kit (JDK) version 1.7 (or later).
3. For Windows OS, the JDK 1.7 has to be installed before running this workflow.

For information about prerequisites for Apache Tomcat, refer to the [Apache Tomcat Product Documentation](#).

How this Workflow Works

This topic contains the following information about the Tomcat - Provision Software workflow:

Validation Checks Performed

The workflow checks the following things prior to extracting the binaries. If any of these checks fails, the workflow fails.

1. All required parameters have values. If any required parameter does not have a value—either a value that you specify or a default value—the workflow fails.
2. Directories and host names are valid. No illegal characters are included. The fully qualified paths specified for downloading Tomcat and Java binaries exist and point to the same folder, for example: `/example/downloads/`.
3. The Java version is 1.7 or later.
4. The operating system is a supported platform.
5. Sufficient disk space is available to extract the binary files from the compressed archive.
6. Sufficient disk space is available to install Tomcat and Java.

Steps Executed

The Tomcat - Provision Software workflow includes the following steps. Each step must complete successfully before the next step can start. If a step fails, the workflow reports a failure, and subsequent steps are skipped.

Process Flow show

This workflow performs the following tasks:

1. Gathers mandatory and optional input parameters (user-provided) to provision Tomcat application server.
2. Validates the parameters needed to provision Tomcat application server.
3. Checks for the existence of a file before downloading.
4. Determines whether the Tomcat application server archive is present on the target server. If not present, the workflow downloads it from the software repository.
5. Extracts the Tomcat application server archive to the specified directories.
6. Validates the extracted files.
7. Updates standalone configuration.
8. Starts Tomcat application server.
9. Discovers Tomcat application server.
10. Cleans up downloaded files that are no longer required, based on user-specified flags in the event of workflow success or failure.

How to Run this Workflow

This topic explains how to customize and run the Tomcat - Provision Software workflow in your environment.

Note: Prior to running this workflow, review the "[Prerequisites for this Workflow](#)", and ensure that all requirements are satisfied.

To customize and run the Tomcat - Provision Software workflow:

1. Create a deployable copy of the workflow.
2. Determine the values that you will specify for the following parameters. These are the parameters that are visible in the deployment by default.

Parameters Defined in this Step: Gather Parameters for Provisioning Tomcat Software

Parameter Name	Default Value	Description
Domain Location	no default	The path to Tomcat domain location.
Download Location	no default	The location where the Java and Tomcat binaries will be downloaded and saved in the target machine.
Install Dir	/opt/tomcat C:\tomcat	Fully qualified path to where the binary files will be uncompressed.
Java Binary Archive	no default	Fully qualified path to where the compressed Java software package should be located on the target machine. The directory should exist on the target machine and must be the same directory specified in the Tomcat Binary Archive parameter. If the Java software package is not available in this directory, then it will be downloaded from the software repository and placed in this directory.
Tomcat Binary Archive	no default	Name of the Tomcat software package. If the Tomcat software package is not available in the target machine, then it will be downloaded from the software repository and placed in Download Location.
Tomcat Group	no default	The user group to which the Tomcat user belongs. This is not supported for Windows OS.
Tomcat Instance Name	no default	Tomcat Instance name that should be provisioned under the given domain as specified by 'Domain Location' parameter.
Tomcat User	no default	The user under which the Tomcat application server will run. The user will be created if not present and the password for the newly created user can be set using 'Tomcat User Password' parameter. If this password is left blank, the 'Tomcat User' value is used as password. This is not supported for Windows OS.

See "[Parameters for Tomcat - Provision Software](#)" for detailed descriptions of all input parameters for this workflow, including default values.

3. In the workflow editor, expose any additional parameters that you need. You will specify values for those parameters when you create the deployment.
4. Save the changes to the workflow (click **Save** in the lower right corner).
5. Create a new deployment.
6. On the Parameters tab, specify values for the required parameters listed in step 2 and any additional parameters that you have exposed. You do not need to specify values for those parameters whose default values are appropriate for your environment.
7. On the Targets tab, specify one or more targets for this deployment.
8. Save the changes to the workflow (click **Save** in the lower right corner).
9. Run the workflow using this deployment.

The workflow will complete and report "Success" on the Console if it has run successfully. If an invalid parameter value is specified, an error is logged, and the workflow terminates in the "Failure" state.

Sample Scenarios

This topic shows you how to use various parameters to achieve the following provisioning scenarios in your environment using the Tomcat - Provision Software workflow:

Specify values for the following parameters to install the Apache Tomcat 8.0. The downloaded Tomcat and Java binaries will be removed upon successful or unsuccessful execution of the workflow.

Step Name	Parameter Name	Example Value
Gather Parameters for Provisioning Tomcat Software	Domain Location	/apps/GTS/domain
	Download Location	/opt/downloads
	Install Dir	/opt/tomcat
	Java Binary Archive	/example/downloads/jdk-7u71-linux-x64.gz
	Tomcat Binary Archive	/example/downloads/apache-tomcat-7.0.64.tar.gz
	Tomcat Group	
	Tomcat Instance Name	tomcatinstance1
	Tomcat User	tomcat
Gather Advanced Parameters for Provisioning Tomcat Software	Clean on Failure	True
	Clean on Success	True
	Custom KeyStore PassPhrase	keystore_password
	Custom KeyStore Path	/opt/tomcat/apache-tomcat-8.0.27/conf/mykeystore.jks
	Custom PrivateKey PassPhrase	pvtkey_password
	Custom TrustStore PassPhrase	truststore_password
	Custom TrustStore Path	/opt/tomcat/apache-tomcat-8.0.27/conf/mytruststore.jks
	Tomcat Admin Password	mypassword
	Tomcat Admin	admin

Step Name	Parameter Name	Example Value
	User	
	Tomcat Instance AJP Port	9009
	Tomcat Instance HTTP Port	18080
	Tomcat Instance SSL Port	18444
	Tomcat User Password	

Be sure that the default values for all remaining parameters (the advanced parameters) are appropriate for your environment.

Parameters for Tomcat - Provision Software

The following tables describe the required and optional input parameters for this workflow. Several of these parameters are not initially visible in a deployment. For many parameters, if you do not specify a value for a parameter, a default value is assigned

Parameters Defined in this Step: Gather Parameters for Provisioning Tomcat Software

Parameter Name	Default Value	Required	Example Value	Description
Domain Location	no default	required	/apps/GTS/domain C:\tomcatdomain	The path to Tomcat domain location.
Download Location	no default	required	/opt/downloads	The location where the Java and Tomcat binaries will be downloaded and saved in the target machine.
Install Dir	/opt/tomcat C:\tomcat	required	/opt/tomcat C:\tomcat	Fully qualified path to where the binary files will be uncompressed.
Java Binary Archive	no default	required	/example/downloads/jdk-7u71-linux-x64.gz	Fully qualified path to where the compressed Java software package should be located on the target machine. The directory should exist on the target machine and must be the same directory specified in the Tomcat Binary Archive parameter. If the Java software package is not available in this directory, then it will be

Parameters Defined in this Step: Gather Parameters for Provisioning Tomcat Software, continued

Parameter Name	Default Value	Required	Example Value	Description
				downloaded from the software repository and placed in this directory.
Tomcat Binary Archive	no default	required	/example/downloads/apache-tomcat-7.0.64.tar.gz	Name of the Tomcat software package. If the Tomcat software package is not available in the target machine, then it will be downloaded from the software repository and placed in Download Location.
Tomcat Group	no default	required		The user group to which the Tomcat user belongs. This is not supported for Windows OS.
Tomcat Instance Name	no default	required	tomcatinstance1	Tomcat Instance name that should be provisioned under the given domain as specified by 'Domain Location' parameter.
Tomcat User	no default	required	tomcat	The user under which the Tomcat application server will run. The user will be created if not present and the password for the newly

Parameters Defined in this Step: Gather Parameters for Provisioning Tomcat Software, continued

Parameter Name	Default Value	Required	Example Value	Description
				created user can be set using 'Tomcat User Password' parameter. If this password is left blank, the 'Tomcat User' value is used as password. This is not supported for Windows OS.

Parameters Defined in this Step: Gather Advanced Parameters for Provisioning Tomcat Software

Parameter Name	Default Value	Required	Example Value	Description
Clean on Failure	True	optional	True	Flag that determines whether to clean up on workflow failure. If set to 'True', the workflow will clean up the downloaded files. Valid values are 'True' and 'False'. The default value is 'True'.
Clean on Success	True	optional	True	Flag that determines whether to clean up on workflow success. If set to 'True', the workflow will clean up the downloaded files. Valid values are 'True' and 'False'. The default value is 'True'.
Custom KeyStore PassPhrase	no default	optional	keystore_password	The password required for the custom keystore, specified as the <i>-storepass</i> argument to the <i>keytool</i> command.
Custom KeyStore Path	no default	optional	/opt/tomcat/apache-tomcat-8.0.27/conf/mykeystore.jks	Fully qualified path to the custom trust store file. If this value is provided, then value

Parameters Defined in this Step: Gather Advanced Parameters for Provisioning Tomcat Software, continued

Parameter Name	Default Value	Required	Example Value	Description
				for the Custom KeyStore PassPhrase and Custom PrivateKey PassPhrase parameters are required. If this field is blank, the SSL will not be enabled in Tomcat.
Custom PrivateKey PassPhrase	no default	optional	pvtkey_password	The password required to retrieve the private key from the keystore, specified as "-keypass" argument to keytool command.
Custom TrustStore PassPhrase	no default	optional	truststore_password	The password required for the custom TrustStore.
Custom TrustStore Path	no default	optional	/opt/tomcat/apache-tomcat-8.0.27/conf/mytruststore.jks	Fully qualified path to the custom TrustStore file.
Tomcat Admin Password	admin	optional	mypassword	Tomcat administrator password which is used to access the Administration Console. The users are maintained in a file called tomcat-users.xml under the conf folder.
Tomcat Admin User	no default	optional	admin	Tomcat administrator user which is used to access the Administration Console. The users are maintained in a file called tomcat-users.xml under the conf folder.
Tomcat Instance AJP Port	no default	optional	9009	Custom AJP port for TomcatInstance.
Tomcat Instance HTTP Port	no default	optional	18080	Custom HTTP port for TomcatInstance.
Tomcat Instance SSL Port	no default	optional	18444	Custom SSL port for TomcatInstance.

Parameters Defined in this Step: Gather Advanced Parameters for Provisioning Tomcat Software, continued

Parameter Name	Default Value	Required	Example Value	Description
				The Keystore details have to be provided in order to enable SSL.
Tomcat User Password	no default	optional		The password for 'Tomcat User' parameter.

Oracle WebLogic

This section includes the following topics:

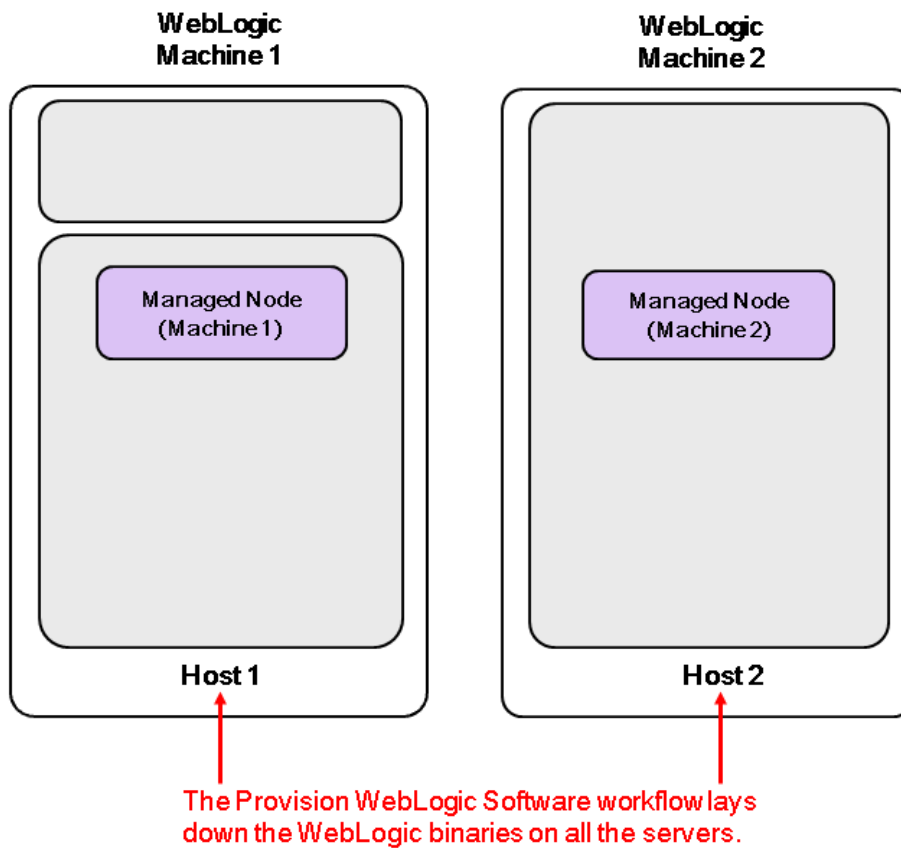
Workflow type	Workflow name
Provisioning	"WebLogic - Provision Weblogic Software" on the next page
	"WebLogic - Provision Weblogic Domain and Admin Server" on page 967
	"WebLogic - Provision Advanced Domain and Admin Server" on page 983
	"WebLogic - Provision Weblogic Managed Servers" on page 996
	"Provision WebLogic Cluster" on page 1015
	"Increase WebLogic Domain Span" on page 1026
	"WebLogic - Create Trust and Identity Keystore" on page 1037
Release Management	"WebLogic - Code Release" on page 1047
Configuring	" WebLogic - Create and Configure Datasource" on page 1060
Patching	"WebLogic - Patch WebLogic Domain v3" on page 1080
	"WebLogic - Rollback Patch" on page 1093

WebLogic - Provision Weblogic Software

This workflow installs a new instance of Oracle WebLogic Server version 11g or 12c onto the target host server (or servers) in silent mode with a response file. Either the native installer (the OS-specific package installer) or generic installer is used.

This workflow supports WebLogic 11g and 12c with either the native installer or the generic installer. The end user specifies whether or not to start the Node Manager. The workflow modifies the Node Manager property file to enable and configure custom SSL connectivity.

The following reference architecture diagram gives an example of what this workflow does:



To use this workflow in your environment, see the following information:

Topic	Information Included
"Prerequisites for this Workflow"	List of prerequisites that must be satisfied before you can run this workflow
"How this Workflow Works"	Information about what the workflow does, including validation checks performed, steps executed, and a high-level process flow
"How to Run this Workflow"	Instructions for running this workflow in your environment
"Sample Scenario"	Examples of typical parameter values for this workflow
Parameters	List of input parameters for this workflow

Note: The documentation for this workflow refers to the workflow and its steps by their base names. The names in the DMA user interface may have a version appended, for example, v2.

Prerequisites for this Workflow

Be sure that the following prerequisites are satisfied before you run the ["WebLogic - Provision Weblogic Software"](#) workflow:

- The latest DMA solution packs require the latest DMA platform. To use the latest solution packs, update the DMA platform. DMA10.50.001.000 solution packs are supported on DMA10.50.001.000 (and later).
- You have installed the Application Server Provisioning Solution Pack.
- You have a support contract and have downloaded the appropriate WebLogic 11g and 12c software to software repository or to the target machine.
- If the generic installer is to be used, you must already have a JDK (Java development kit)—supported by the version of WebLogic 11g and 12c you are installing—installed on the target machine.

Memory

A minimum of 1 GB RAM, although Oracle recommends 2 GB of RAM.

Hard disk drive

A complete installation (including SDKs) requires approximately 3.9 GB of disk space. This includes temporary disk space that is needed during installation. Depending on the components you choose to install, and the installer that you are using, less disk space may be needed.

Processor

1-GHz (or faster) CPU

For more information about prerequisites for WebLogic 11g and 12c, refer to the [WebLogic Product Documentation](#).

How this Workflow Works

The following information describes how the "WebLogic - Provision Weblogic Software" workflow works:

Overview

The workflow does the following:

- Prepares to provision the WebLogic 11g and 12c software on all target machines by setting up the command to be used in subsequent steps, validating input parameters, verifying that the operating system is supported, and determining that enough temporary storage space is available.
- Checks the existence of the binary executable file, downloads it from the software repository if it doesn't exist, then changes the file ownership and permissions so that it can be executed.
- Creates the response file that is required to drive the WebLogic 11g and 12c installation.
- Depending on the Java Home parameter:

If the Java Home parameter is specified, the workflow uses the generic package installer—the JDK utility located at Java Home—to lay down the WebLogic 11g and 12c binaries onto the target host server using silent mode and the specified response file.

If the Java Home parameter is not specified, the workflow uses the OS-specific package installer to lay down the WebLogic 11g and 12c binaries onto the target host server using silent mode and the specified response file.

- *Optional:* Starts the WebLogic 11g and 12c Node Manager process on the target host servers.
- *Optional:* Configures the Custom SSL configurations for the WebLogic 11g and 12c Node Manager. Stops and restarts the WebLogic 11g and 12c Node Manager to apply the SSL configuration changes.
- Cleans up any files that were downloaded—for either workflow success or failure.

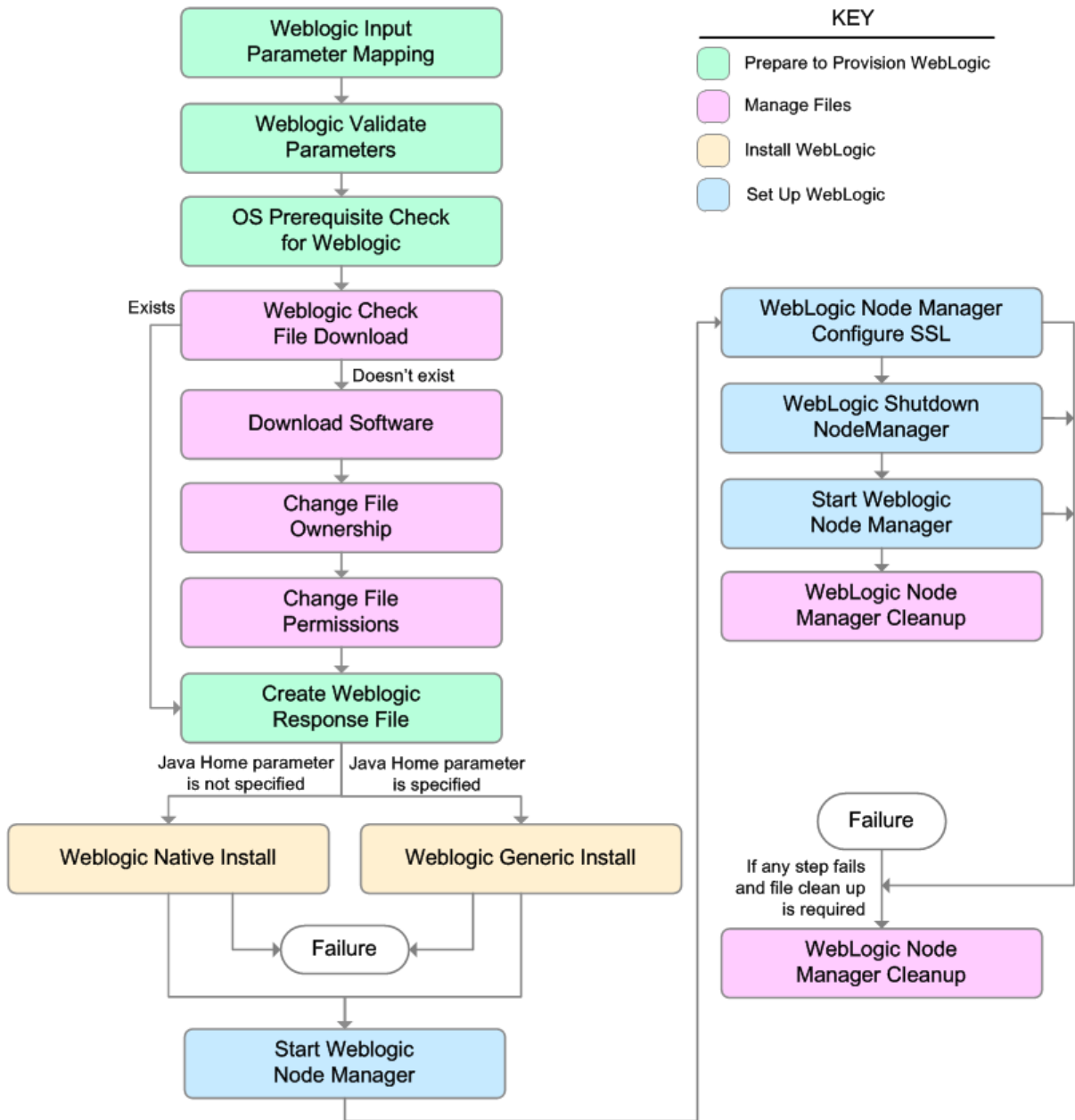
Validation Checks Performed

Much of the validation centers on the input parameters:

- Required parameters have values specified.
- The Binary Archive file or path is valid.
- The Java Home, Staging Directory, NM Log File are valid.
- The Node Manager Service, Setup Custom SSL Stores, and Start Node Manager parameters are either true or false.
- The Node Manager Port is either null or a valid integer.
- The Binary Archive and Java Home are valid install files.
- If Setup Custom SSL Stores is true, the following parameters are specified: Custom KeyStore PassPhrase, Custom KeyStore Path, Custom KeyStore Type, Custom PrivateKey PassPhrase, Custom TrustStore Path, and Private Key Alias.
- The WebLogic User and WebLogic Group exist and the WebLogic User is part of the specified WebLogic Group.

Steps Executed

The WebLogic - Provision Weblogic Software workflow includes the following steps. Each step must complete successfully before the next step can start. If a step fails, the workflow reports a failure and all subsequent steps are skipped.



Steps Used in WebLogic - Provision Weblogic Software

Workflow Step	Description
Weblogic	This step performs the following actions to facilitate the execution of subsequent

Steps Used in WebLogic - Provision Weblogic Software, continued

Workflow Step	Description
Input Parameter Mapping	<p>steps in the workflow:</p> <ol style="list-style-type: none"> 1. Sets the Call Wrapper parameter to its default value. The Call Wrapper is the command that executes a step as a specific user. 2. Allows certain parameters— that may or may not be required depending on what type of action you want to perform—to be hidden or exposed.
Weblogic Validate Parameters	This step prepares and validates the input parameters required to install WebLogic 11g and 12c.
OS Prerequisite Check for Weblogic	This step first determines whether the operating system kernel on the target server is a supported version, and then it determines if adequate temporary space is available to extract the contents of the installation binaries and install WebLogic 11g and 12c.
Weblogic Check File Download	<p>This step checks for the existence of a file on the target machine before downloading that file from the software repository. For each file in the specified File List, it:</p> <ol style="list-style-type: none"> 1. Determines whether the file is in the expected location on the target machine. 2. If the file is not in the expected location, adds that file to a list of files that need to be downloaded.
Download Software	This step downloads a list of files to a specified location on the target server.
Change File Ownership	This step changes the ownership of a comma-delimited list of files to the specified user and group.
Change File Permissions	This step changes the permissions settings for one or more specified files or directories.
Create Weblogic Response File	This step creates the response file required to drive the installation of WebLogic 11g and 12c and determines whether the generic or native installer will be used.
Weblogic Native Install	This step starts the installation of WebLogic 11g and 12c using the native installer—OS-package specific—with silent mode and the specified response file.
Weblogic Generic Install	This step starts the installation of WebLogic 11g and 12c using the generic installer—JDK utility—with silent mode and the specified response file.
Start Weblogic Node Manager	This step checks if Start Node Manager is set to true. If so, it starts the WebLogic 11g and 12c Node Manager process on the target server. Then the step verifies that the Node Manager started.
WebLogic Node Manager Configure SSL	This step updates the <code>nodemanager.properties</code> file with the SSL configurations and changes the Node Manager log file location.

Steps Used in WebLogic - Provision Weblogic Software, continued

Workflow Step	Description
WebLogic Shutdown NodeManager	This step stops the WebLogic 11g and 12c Node Manager on a given machine or server.
Start Weblogic Node Manager	This step checks if Start Node Manager is set to true. If so, it starts the WebLogic 11g and 12c Node Manager process on the target server. Then the step verifies that the Node Manager started.
WebLogic Node Manager Cleanup	This step removes all temporary downloaded files and archives.

For parameter descriptions and defaults, see ["Parameters for WebLogic - Provision Weblogic Software"](#).

How to Run this Workflow

The following instructions show you how to customize and run the ["WebLogic - Provision Weblogic Software"](#) workflow in your environment.

The workflow provides default values for some parameters. These default values are usually sufficient for a "typical" installation. You can override the defaults by specifying parameter values in the deployment. You can also expose additional parameters in the workflow, if necessary, to accomplish more advanced scenarios. Any parameters not explicitly specified in the deployment will have the default values listed in ["Parameters for WebLogic - Provision Weblogic Software"](#).

Note: Before following this procedure, review the ["Prerequisites for this Workflow"](#) on page 952, and ensure that all requirements are satisfied.

To use the WebLogic - Provision Weblogic Software workflow:

1. Create a deployable copy of the workflow.
2. Determine the values that you will specify for the following parameters:

Input Parameters for Weblogic Validate Parameters

Parameter Name	Default Value	Required	Description
BEA Home	no default	required	Fully qualified path to the middleware home directory that will contain this installation. For example: /opt/oracle/weblogic
Binary Archive	no default	required	Fully qualified path to the WebLogic Package Installer. Not required if Java Binary Archive is provided.
Component Paths	see description	required	<p>The components and/or subcomponents that you want to install on your system. To install multiple components, separate the components with a bar character. Default is:</p> <p>WebLogic Server/Core Application Server WebLogic Server/Administration Console WebLogic Server/Configuration Wizard and Upgrade Framework WebLogic Server/Web 2.0 HTTP Pub-Sub Server WebLogic Server/WebLogic JDBC Drivers WebLogic Server/Third Party JDBC Drivers WebLogic Server/WebLogic Server Clients WebLogic Server/WebLogic Web Server Plugins WebLogic Server/UDDI and Xquery Support WebLogic Server/Server Examples</p> <p>Note: If you specify WebLogic Server, you will install all of the above.</p>

Input Parameters for Weblogic Validate Parameters, continued

Parameter Name	Default Value	Required	Description
Java Home	no default	required if generic installer is used	Fully qualified path to the JAVA_HOME—JDK utility—that will be used for the generic install. For example: <code>/opt/oracle/jdk1.6.0_35</code>
Log File	no default	required	The fully qualified path where a verbose log file will be generated during installation. For example: <code>/var/tmp/weblogic_log.txt</code>
Setup Custom SSL Stores	no default	required	Determines whether you want to run Secure Socket Layer (SSL) with the demo SSL certificates or with your own custom keystore and truststore. Valid values are true or false. If Setup Custom SSL Stores is true, the following parameters must also be specified: Custom KeyStore PassPhrase, Custom KeyStore Path, Custom KeyStore Type, Custom PrivateKey PassPhrase, Custom TrustStore Path, and Private Key Alias.
Staging Directory	no default	required	Fully qualified path to a temporary directory that the installer will use to uncompress the binary into.
Start Node Manager	true	required	Determines whether to start the WebLogic 11g and 12c Node Manager. Valid values are true and false.
WLS Install Home	no default	required	Fully qualified path to the directory where WebLogic Server will be installed. For example: <code>/opt/oracle/weblogic/wlserver12.1</code>
Weblogic Group	see description	optional	Group ID used to install the WebLogic 11g and 12c software. The default is the group ID of root.
Weblogic User	root	optional	User ID used to install the WebLogic 11g and 12c software.

Note: This is the minimum set of parameters required to run this workflow. You may need to expose additional parameters depending on your objectives.

See ["Parameters for WebLogic - Provision Weblogic Software"](#) for detailed descriptions of all input parameters for this workflow, including default values.

3. In the workflow editor, expose any additional parameters that you need. You will specify values for those parameters when you create the deployment.
4. Save the changes to the workflow (click **Save** in the lower right corner).
5. Create a new deployment.
6. On the Parameters tab, specify values for the required parameters listed in step 2 and any

additional parameters that you have exposed. You do not need to specify values for those parameters whose default values are appropriate for your environment.

7. On the Targets tab, specify one or more targets for this deployment.

Note: The target for this deployment should be set to all the servers that are involved in your WebLogic 11g and 12c installation.

8. Save the deployment (click **Save** in the lower right corner).
9. Run the workflow using this deployment.

To verify the results:

The workflow will complete and report SUCCESS on the Console if it has run successfully. If an error occurs during the workflow execution, the error will be logged, and the workflow terminates in the FAILURE state.

Optional: If you want to further verify the results:

View the `{BEAHOME}/logs/log.txt` file. This file is created after the installation and contains specific information about what was installed.

Sample Scenario

This topic shows you typical parameter values for different use cases for the ["WebLogic - Provision Weblogic Software"](#) workflow.

Scenario 1: Use the native installer and install WebLogic 11g and 12c as a non-root user

If you want to use the native—OS-specific—package installer to lay down the WebLogic 11g and 12c binaries onto the target host server, do not set the Java Home parameter.

Set Setup Custom SSL Stores to false.

Input Parameters for Weblogic Validate Parameters

Parameter Name	Example Value	Description
BEA Home	see description	Fully qualified path to the middleware home directory that will contain this installation. For example: <code>/opt/oracle/weblogic</code>
Binary Archive	<code>wls_1035_linux.bin</code>	Fully qualified path to the WebLogic Package Installer. Not required if Java Binary Archive is provided.
Component Paths	WebLogic Server (this installs everything under it)	<p>The components and/or subcomponents that you want to install on your system. To install multiple components, separate the components with a bar character. Default is:</p> <p>WebLogic Server/Core Application Server WebLogic Server/Administration Console WebLogic Server/Configuration Wizard and Upgrade Framework WebLogic Server/Web 2.0 HTTP Pub-Sub Server WebLogic Server/WebLogic JDBC Drivers WebLogic Server/Third Party JDBC Drivers WebLogic Server/WebLogic Server Clients WebLogic Server/WebLogic Web Server Plugins WebLogic Server/UDDI and Xquery Support WebLogic Server/Server Examples</p> <p>Note: If you specify WebLogic Server, you will install all of the above.</p>
Java Home		Fully qualified path to the JAVA_HOME—JDK utility—that will be used for the generic install. For example: <code>/opt/oracle/jdk1.6.0_35</code>
Log File		The fully qualified path where a verbose log file will be generated during installation. For example: <code>/var/tmp/weblogic_log.txt</code>
Setup Custom SSL Stores	false	Determines whether you want to run Secure Socket Layer (SSL) with the demo SSL certificates or with your own custom keystore and truststore. Valid values are true or false.

Input Parameters for Weblogic Validate Parameters, continued

Parameter Name	Example Value	Description
		If Setup Custom SSL Stores is true, the following parameters must also be specified: Custom KeyStore PassPhrase, Custom KeyStore Path, Custom KeyStore Type, Custom PrivateKey PassPhrase, Custom TrustStore Path, and Private Key Alias.
Staging Directory	/tmp/	Fully qualified path to a temporary directory that the installer will use to uncompress the binary into.
Start Node Manager	true	Determines whether to start the WebLogic 11g and 12c Node Manager. Valid values are true and false.
WLS Install Home	see description	Fully qualified path to the directory where WebLogic Server will be installed. For example: /opt/oracle/weblogic/wlserver12.1
Weblogic Group	wlgrp	Group ID used to install the WebLogic 11g and 12c software. The default is the group ID of root.
Weblogic User	wlsuser	User ID used to install the WebLogic 11g and 12c software.

Be sure that the default values for all remaining input parameters are appropriate for your environment (see ["Parameters for WebLogic - Provision Weblogic Software"](#)).

Scenario 2: Use the generic installer, configure SSL with a custom keystore and truststore, and install WebLogic 11g and 12c as a non-root user

If you want to use the generic package installer to lay down the WebLogic 11g and 12c binaries onto the target host server, set the Java Home parameter to the JDK utility location.

Use this case to set up SSL to have the Node Manager communicate via SSL. Set Setup Custom SSL Stores to true. Also provide values for the following parameters: Custom KeyStore PassPhrase, Custom KeyStore Path, Custom KeyStore Type, Custom PrivateKey PassPhrase, Custom TrustStore Path, and Private Key Alias.

Input Parameters for Weblogic Validate Parameters

Parameter Name	Example Value	Description
BEA Home	see description	Fully qualified path to the middleware home directory that will contain this installation. For example: <code>/opt/oracle/weblogic</code>
Binary Archive	<code>wls_1035_linux.bin</code>	Fully qualified path to the WebLogic Package Installer. Not required if Java Binary Archive is provided.
Component Paths	WebLogic Server (this installs everything under it)	The components and/or subcomponents that you want to install on your system. To install multiple components, separate the components with a bar character. Default is: WebLogic Server/Core Application Server WebLogic Server/Administration Console WebLogic Server/Configuration Wizard and Upgrade Framework WebLogic Server/Web 2.0 HTTP Pub-Sub Server WebLogic Server/WebLogic JDBC Drivers WebLogic Server/Third Party JDBC Drivers WebLogic Server/WebLogic Server Clients WebLogic Server/WebLogic Web Server Plugins WebLogic Server/UDDI and Xquery Support WebLogic Server/Server Examples Note: If you specify WebLogic Server, you will install all of the above.
Custom KeyStore PassPhrase	password	Password for the custom keystore.
Custom KeyStore Path	<code>/opt/WebLogic/keystore</code>	Fully qualified path to the custom keystore file.
Custom KeyStore Type	JKS	The type of the Identity keystore.
Custom PrivateKey PassPhrase	password	Password used to retrieve the private key for the WebLogic 11g and 12c Server from the Identity keystore.

Input Parameters for WebLogic Validate Parameters, continued

Parameter Name	Example Value	Description
Custom TrustStore Path	/opt/WebLogic/truststore	Fully qualified path to the custom truststore file.
Java Home	see description	Fully qualified path to the JAVA_HOME—JDK utility—that will be used for the generic install. For example: /opt/oracle/jdk1.6.0_35
Log File	/tmp/weblogic_log.txt	The fully qualified path where a verbose log file will be generated during installation. For example: /var/tmp/weblogic_log.txt
Private Key Alias	Hostname	The keystore attribute that defines the string alias used to store and retrieve the server's private key.
Setup Custom SSL Stores	true	Determines whether you want to run Secure Socket Layer (SSL) with the demo SSL certificates or with your own custom keystore and truststore. Valid values are true or false. If Setup Custom SSL Stores is true, the following parameters must also be specified: Custom KeyStore PassPhrase, Custom KeyStore Path, Custom KeyStore Type, Custom PrivateKey PassPhrase, Custom TrustStore Path, and Private Key Alias.
Staging Directory	/tmp/	Fully qualified path to a temporary directory that the installer will use to uncompress the binary into.
Start Node Manager	true	Determines whether to start the WebLogic 11g and 12c Node Manager. Valid values are true and false.
WLS Install Home	see description	Fully qualified path to the directory where WebLogic Server will be installed. For example: /opt/oracle/weblogic/wlserver12.1
Weblogic Group	wlsgrp	Group ID used to install the WebLogic 11g and 12c software. The default is the group ID of root.
Weblogic User	wlsuser	User ID used to install the WebLogic 11g and 12c software.

Note: Some of these parameters are not exposed by default in the deployment.

You need to expose the following parameters: Custom KeyStore PassPhrase, Custom KeyStore Path, Custom KeyStore Type, Custom PrivateKey PassPhrase, Custom TrustStore Path, Node Manager Service, and Private Key Alias.

Be sure that the default values for all remaining input parameters are appropriate for your environment (see ["Parameters for WebLogic - Provision Weblogic Software"](#)).

Parameters for WebLogic - Provision Weblogic Software

The following tables describe the required and optional input parameters for this workflow. Some of these parameters may not be initially visible in a deployment. For some parameters, if you do not specify a value for a parameter, a default value is assigned.

Following is a table for the sole step used by this workflow where parameters are defined:

Parameters Defined in this Step: Weblogic Validate Parameters

Parameter Name	Default Value	Required	Description
BEA Home	no default	required	Fully qualified path to the middleware home directory that will contain this installation. For example: /opt/oracle/weblogic
Binary Archive	no default	required	Fully qualified path to the WebLogic Package Installer. Not required if Java Binary Archive is provided.
Component Paths	see description	required	<p>The components and/or subcomponents that you want to install on your system. To install multiple components, separate the components with a bar character. Default is:</p> <p>WebLogic Server/Core Application Server WebLogic Server/Administration Console WebLogic Server/Configuration Wizard and Upgrade Framework WebLogic Server/Web 2.0 HTTP Pub-Sub Server WebLogic Server/WebLogic JDBC Drivers WebLogic Server/Third Party JDBC Drivers WebLogic Server/WebLogic Server Clients WebLogic Server/WebLogic Web Server Plugins WebLogic Server/UDDI and Xquery Support WebLogic Server/Server Examples</p> <p>Note: If you specify WebLogic Server, you will install all of the above.</p>
Custom KeyStore PassPhrase	no default	optional	Password for the custom keystore.
Custom KeyStore Path	no default	optional	Fully qualified path to the custom keystore file.
Custom KeyStore Type	JKS	optional	The type of the Identity keystore.
Custom PrivateKey PassPhrase	no default	optional	Password used to retrieve the private key for the WebLogic 11g and 12c Server from the Identity keystore.
Custom TrustStore	no default	optional	Fully qualified path to the custom truststore file.

Parameters Defined in this Step: Weblogic Validate Parameters, continued

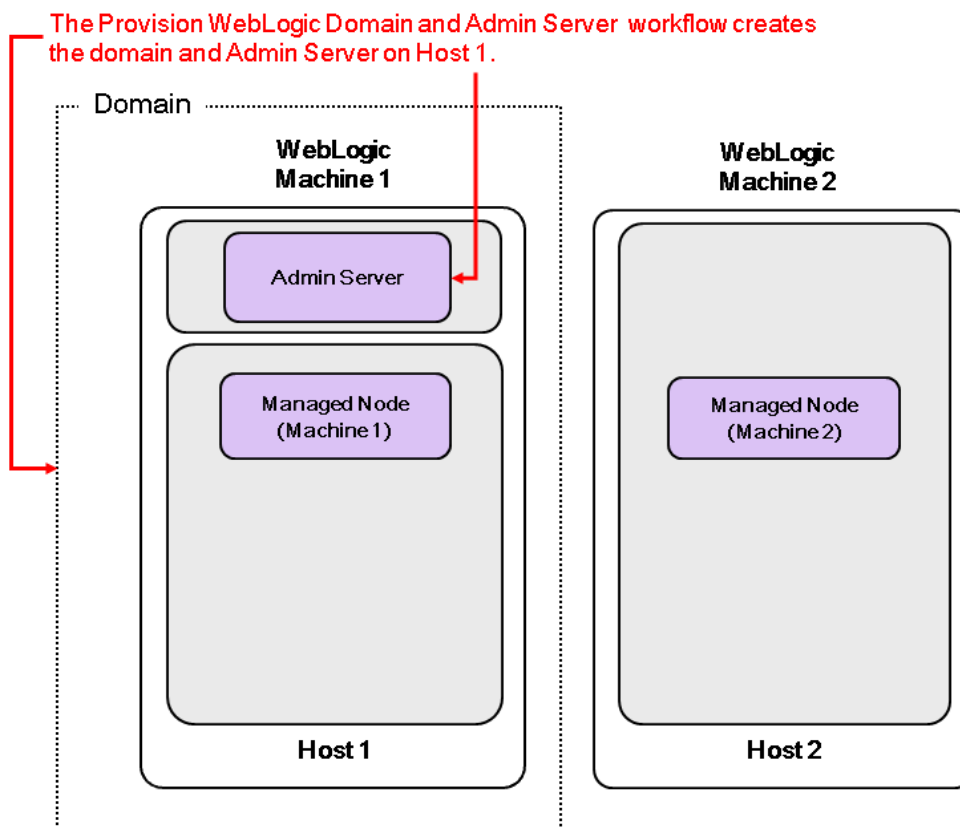
Parameter Name	Default Value	Required	Description
Path			
Java Home	no default	required if generic installer is used	Fully qualified path to the JAVA_HOME—JDK utility—that will be used for the generic install. For example: /opt/oracle/jdk1.6.0_35
Log File	no default	required	The fully qualified path where a verbose log file will be generated during installation. For example: /var/tmp/weblogic_log.txt
NM Log File	no default	optional	The fully qualified path where a Node Manager log file will be generated during installation.
Node Manager Port	5556	optional	Sets the port number under which the Node Manager will run.
Node Manager Service	false	required	Provides the option to set the Node Manager to run as a Windows Service. Valid values are true or false.
Private Key Alias	no default	optional	The keystore attribute that defines the string alias used to store and retrieve the server's private key.
Setup Custom SSL Stores	no default	required	Determines whether you want to run Secure Socket Layer (SSL) with the demo SSL certificates or with your own custom keystore and truststore. Valid values are true or false. If Setup Custom SSL Stores is true, the following parameters must also be specified: Custom KeyStore PassPhrase, Custom KeyStore Path, Custom KeyStore Type, Custom PrivateKey PassPhrase, Custom TrustStore Path, and Private Key Alias.
Staging Directory	no default	required	Fully qualified path to a temporary directory that the installer will use to uncompress the binary into.
Start Node Manager	true	required	Determines whether to start the WebLogic 11g and 12c Node Manager. Valid values are true and false.
WLS Install Home	no default	required	Fully qualified path to the directory where WebLogic Server will be installed. For example: /opt/oracle/weblogic/wlserver12.1
Weblogic Group	see description	optional	Group ID used to install the WebLogic 11g and 12c software. The default is the group ID of root.
Weblogic User	root	optional	User ID used to install the WebLogic 11g and 12c software.

WebLogic - Provision Weblogic Domain and Admin Server

This workflow creates a WebLogic domain and Administration Server from an existing installation of WebLogic 11g or 12c.

After you have the WebLogic 11g or 12c binaries installed, this workflow sets up the process server and creates the domain where the components can be placed.

The following reference architecture diagram gives an example of what this workflow does:



To use this workflow in your environment, see the following information:

Topic	Information Included
"Prerequisites for this Workflow"	List of prerequisites that must be satisfied before you can run this workflow
"How this Workflow Works"	Information about what the workflow does, including validation checks performed, steps executed, and a high-level process flow
"How to Run this Workflow"	Instructions for running this workflow in your environment
"Sample Scenario"	Examples of typical parameter values for this workflow
Parameters	List of input parameters for this workflow.

Note: The documentation for this workflow contains steps that are referred to by their base names. The names in the DMA user interface may have a version appended, for example, v2.

Prerequisites for this Workflow

Be sure that the following prerequisites are satisfied before you run the ["WebLogic - Provision Weblogic Domain and Admin Server"](#) workflow:

1. The latest DMA solution packs require the latest DMA platform. To use the latest solution packs, update the DMA platform. DMA10.50.001.000 solution packs are supported on DMA10.50.001.000 (and later).
2. You have installed the Application Server Provisioning Solution Pack.

For more information about prerequisites for WebLogic 11g and 12c, refer to the [WebLogic Product Documentation](#).

How this Workflow Works

The following information describes how the "WebLogic - Provision Weblogic Domain and Admin Server" workflow works:

Overview

The workflow does the following:

- Prepares to provision the WebLogic 11g and 12c domain and Administration Server by setting up the command to be used in subsequent steps and validating input parameters.
- Creates the domain and Administration Server using the WebLogic Scripting Tool (WLST). To do this the workflow opens a domain template, configures the Administration Server and SSL port, writes the domain, then closes the domain template.
- Starts the WebLogic 11g and 12c Administration Manager process on the target host server.

Validation Checks Performed

Much of the validation centers on the input parameters:

- Verifies that required parameters have values specified.
- Checks that the BEA Home and WLS Install Home files exist.
- Verifies that Admin Server Port and Admin SSL Port are null or valid integers.
- Verifies that Enable SSL, Setup Custom SSL Stores, and Start Node Manager are either true or false.
- Verifies that if Enable SSL is true that Setup Custom SSL Stores is also true.
- Verifies that if Enable SSL is true that Admin SSL Port has a value and if Enable SSL is false that Admin SSL Port does not have a value.
- If Setup Custom SSL Stores is true:

Verifies that the following are specified: Custom KeyStore PassPhrase, Custom KeyStore Path, Custom KeyStore Type, Custom TrustStore PassPhrase, Custom TrustStore Path.

Verifies that Custom KeyStore Path and Custom TrustStore Path are null or the paths exist.

Steps Executed

The WebLogic - Provision Weblogic Domain and Admin Server workflow includes the following steps. Each step must complete successfully before the next step can start. If a step fails, the workflow reports a failure and all subsequent steps are skipped.



Steps Used in WebLogic - Provision Weblogic Domain and Admin Server

Workflow Step	Description
Get WebLogic Call-Wrappers	This step creates the commands that subsequent steps will use to execute scripts and WebLogic 11g and 12c Scripting Tool (WLST) operations.
Weblogic Domain Admin Server Validate Parameters	This step prepares and validates the parameters needed to create a WebLogic 11g and 12c domain and Administration Server.
Create Weblogic Domain Admin Server	This step creates a WebLogic 11g and 12c domain and Administration Server. Optionally, the step configures SSL custom keystore and truststore. Optionally, the step enables SSL.
Start Weblogic Node Manager	This step checks if Start Node Manager is set to true. If so, it starts the WebLogic 11g and 12c Node Manager process on the target server. Then the step verifies that the Node Manager started.
Start Weblogic Admin Server	This step starts the WebLogic 11g and 12c Administration Server.

For parameter descriptions and defaults, see ["Parameters for WebLogic - Provision Weblogic Domain and Admin Server"](#).

How to Run this Workflow

The following instructions show you how to customize and run the ["WebLogic - Provision Weblogic Domain and Admin Server"](#) workflow in your environment.

The workflow provides default values for some parameters. These default values are usually sufficient for a "typical" installation. You can override the defaults by specifying parameter values in the deployment. You can also expose additional parameters in the workflow, if necessary, to accomplish more advanced scenarios. Any parameters not explicitly specified in the deployment will have the default values listed in ["Parameters for WebLogic - Provision Weblogic Domain and Admin Server"](#).

Note: Before following this procedure, review the ["Prerequisites for this Workflow"](#) on page 969, and ensure that all requirements are satisfied.

To use the WebLogic - Provision Weblogic Domain and Admin Server workflow:

1. Create a deployable copy of the workflow.
2. Determine the values that you will specify for the following parameters:

Input Parameters for Get WebLogic Call-Wrappers

Parameter Name	Default Value	Required	Description
BEA Home	no default	required	Fully qualified path to the middleware home directory that contains the WebLogic 11g and 12c installation. For example: /opt/oracle/weblogic
WLS Install Home	no default	required	Fully qualified path to the directory where WebLogic Server will be installed. For example: /opt/oracle/weblogic/wlserver12.1

Input Parameters for Weblogic Domain Admin Server Validate Parameters

Parameter Name	Default Value	Required	Description
Admin Server Name	no default	required	Label or name given to the Administration Server.
Admin Server Port	no default	required	The non-SSL port on which the WebLogic 11g and 12c Administration Server will run.
Domain Path	no default	required	Fully qualified path where the domain and domain configuration will be created. For example: /opt/weblogic/user_projects/domains

Input Parameters for Weblogic Domain Admin Server Validate Parameters, continued

Parameter Name	Default Value	Required	Description
Enable SSL	false	required	Tells the WebLogic 11g and 12c Administration Server to either use (true) or not use (false) the SSL port for communication.
Setup Custom SSL Stores	no default	required	Determines whether you want to run Secure Socket Layer (SSL) with the demo SSL certificates or with your own custom keystore and truststore. Valid values are true or false. If Setup Custom SSL Stores is true, the following parameters must also be specified: Custom KeyStore PassPhrase, Custom KeyStore Path, Custom KeyStore Type, Custom TrustStore PassPhrase, Custom TrustStore Path, and Private Key Alias.
Start Node Manager	true	required	Determines whether to start the WebLogic 11g and 12c Node Manager. Valid values are true and false.
Weblogic Admin Password	no default	required	The password that will be used to authenticate with the WebLogic 11g and 12c Administration Server.

Tip: To avoid having to re-enter passwords whenever they change, you can create a policy to provide them to the workflow.

Note: See "[Parameters for WebLogic - Provision Weblogic Domain and Admin Server](#)" for detailed descriptions of all input parameters for this workflow, including default values.

- In the workflow editor, expose any additional parameters that you need. You will specify values for those parameters when you create the deployment.
- Save the changes to the workflow (click **Save** in the lower right corner).
- Create a new deployment.
- On the Parameters tab, specify values for the required parameters listed in step 2 and any additional parameters that you have exposed. You do not need to specify values for those parameters whose default values are appropriate for your environment.
- On the Targets tab, specify one or more targets for this deployment.

Note: The target for this deployment should be set to the server where the WebLogic 11g and 12c Administration Server will be provisioned.

- Save the deployment (click **Save** in the lower right corner).
- Run the workflow using this deployment.

To verify the results:

The workflow will complete and report SUCCESS on the Console if it has run successfully. If an error occurs during the workflow execution, the error will be logged, and the workflow terminates in the FAILURE state.

Optional: If you want to further verify the results:

1. View the {DomainPath}/servers/AdminServer/logs/AdminServer.log file.

This file is created when the Admin Server is started up.

2. Look for the following to see if the Admin Server started up cleanly:

Server started in RUNNING mode.

Sample Scenario

This topic shows you typical parameter values for different use cases for the "[WebLogic - Provision Weblogic Domain and Admin Server](#)" workflow.

Scenario 1: Create a Domain and Administration Server without configuring or enabling SSL

Set Setup Custom SSL Stores and Enable SSL to false.

Input Parameters for Get WebLogic Call-Wrappers

Parameter Name	Example Value	Description
BEA Home	see description	Fully qualified path to the middleware home directory that contains the WebLogic 11g and 12c installation. For example: <code>/opt/oracle/weblogic</code>
WLS Install Home	see description	Fully qualified path to the directory where WebLogic Server will be installed. For example: <code>/opt/oracle/weblogic/wlserver12.1</code>

Input Parameters for Weblogic Domain Admin Server Validate Parameters

Parameter Name	Example Value	Description
Admin Server Name	myAdminServer	Label or name given to the Administration Server.
Admin Server Port	8001	The non-SSL port on which the WebLogic 11g and 12c Administration Server will run.
Domain Path	see description	Fully qualified path where the domain and domain configuration will be created. For example: <code>/opt/weblogic/user_projects/domains</code>
Enable SSL	false	Tells the WebLogic 11g and 12c Administration Server to either use (true) or not use (false) the SSL port for communication.
Setup Custom SSL Stores	false	Determines whether you want to run Secure Socket Layer (SSL) with the demo SSL certificates or with your own custom keystore and truststore. Valid values are true or false. If Setup Custom SSL Stores is true, the following parameters must also be specified: Custom KeyStore PassPhrase, Custom KeyStore Path, Custom KeyStore Type, Custom TrustStore PassPhrase, Custom TrustStore Path, and Private Key Alias.
Start Node Manager	true	Determines whether to start the WebLogic 11g and 12c Node Manager. Valid values are true and false.
Weblogic Admin Password	password	The password that will be used to authenticate with the WebLogic 11g and 12c Administration Server.

Be sure that the default values for all remaining input parameters are appropriate for your environment (see "[Parameters for WebLogic - Provision Weblogic Domain and Admin Server](#)").

Scenario 2: Create a Domain and Administration Server and configure and enable SSL

Use this case to set up SSL to have the Node Manager communicate via SSL. Set Setup Custom SSL Stores to true. Also provide values for the following parameters: Custom KeyStore Path, Custom KeyStore PassPhrase, Custom TrustStore Path, Custom TrustStore PassPhrase, and Private Key Alias.

If you want to enable the SSL port for communication set Enable SSL to true and set Admin SSL Port to the port number.

Input Parameters for Get WebLogic Call-Wrappers

Parameter Name	Example Value	Description
BEA Home	see description	Fully qualified path to the middleware home directory that contains the WebLogic 11g and 12c installation. For example: <code>/opt/oracle/weblogic</code>
WLS Install Home	see description	Fully qualified path to the directory where WebLogic Server will be installed. For example: <code>/opt/oracle/weblogic/wlserver12.1</code>

Input Parameters for Weblogic Domain Admin Server Validate Parameters

Parameter Name	Example Value	Description
Admin SSL Port	8002	The Secure Sockets Layer (SSL) port on which the WebLogic 11g and 12c Administration Server will run. If Enable SSL is set to true, this parameter must also have a value.
Admin Server Name	myAdminServer	Label or name given to the Administration Server.
Admin Server Port	8001	The non-SSL port on which the WebLogic 11g and 12c Administration Server will run.
Custom KeyStore PassPhrase	password	Password for the custom keystore.
Custom KeyStore Path	<code>/opt/WebLogic/keystore</code>	Fully qualified path to the custom keystore file.
Custom KeyStore Type	JKS	The type of the Identity keystore.
Custom TrustStore PassPhrase	password	Password for the custom truststore.
Custom TrustStore	<code>/opt/WebLogic/truststore</code>	Fully qualified path to the custom truststore file.

Input Parameters for Weblogic Domain Admin Server Validate Parameters, continued

Parameter Name	Example Value	Description
Path		
Domain Path	see description	Fully qualified path where the domain and domain configuration will be created. For example: <code>/opt/weblogic/user_projects/domains</code>
Enable SSL	true	Tells the WebLogic 11g and 12c Administration Server to either use (true) or not use (false) the SSL port for communication.
Private Key Alias	Hostname	The keystore attribute that defines the string alias used to store and retrieve the server's private key.
Setup Custom SSL Stores	true	Determines whether you want to run Secure Socket Layer (SSL) with the demo SSL certificates or with your own custom keystore and truststore. Valid values are true or false. If Setup Custom SSL Stores is true, the following parameters must also be specified: Custom KeyStore PassPhrase, Custom KeyStore Path, Custom KeyStore Type, Custom TrustStore PassPhrase, Custom TrustStore Path, and Private Key Alias.
Start Node Manager	true	Determines whether to start the WebLogic 11g and 12c Node Manager. Valid values are true and false.
Weblogic Admin Password	password	The password that will be used to authenticate with the WebLogic 11g and 12c Administration Server.

Note: Some of these parameters are not exposed by default in the deployment.

You need to expose the following parameters: Admin SSL Port, Custom KeyStore PassPhrase, Custom KeyStore Path, Custom KeyStore Type, Custom TrustStore PassPhrase, and Custom TrustStore Path.

Be sure that the default values for all remaining input parameters are appropriate for your environment (see "[Parameters for WebLogic - Provision Weblogic Domain and Admin Server](#)").

Parameters for WebLogic - Provision Weblogic Domain and Admin Server

The following tables describe the required and optional input parameters for this workflow. Some of these parameters may not be initially visible in a deployment. For some parameters, if you do not specify a value for a parameter, a default value is assigned.

Following are tables for each of the steps used by this workflow where parameters are defined:

Parameters Defined in this Step: Get WebLogic Call-Wrappers

Parameter Name	Default Value	Required	Description
BEA Home	no default	required	Fully qualified path to the middleware home directory that contains the WebLogic 11g and 12c installation. For example: <code>/opt/oracle/weblogic</code>
WLS Install Home	no default	required	Fully qualified path to the directory where WebLogic Server will be installed. For example: <code>/opt/oracle/weblogic/wlserver12.1</code>

Additional Parameters Defined in this Step: Weblogic Domain Admin Server Validate Parameters

Parameter Name	Default Value	Required	Description
Admin SSL Port	no default	optional	The Secure Sockets Layer (SSL) port on which the WebLogic 11g and 12c Administration Server will run. If Enable SSL is set to true, this parameter must also have a value.
Admin Server Hostname	Server.name	required	The WebLogic 11g and 12c Administration Server host name or IP address that the Administration Server will run on. The Administration Server is used to issue administrative commands to the Application Servers.
Admin Server Name	no default	required	Label or name given to the Administration Server.
Admin Server Port	no default	required	The non-SSL port on which the WebLogic 11g and 12c Administration Server will run.
Call Wrapper	see description	required	<p>Command that will execute this step (or subsequent steps) as a specific user.</p> <p>For UNIX targets, the default is: <code>/opt/hp/dma/client/jython.sh</code> running as root</p> <p>For Windows targets, the default is: jython running as Administrator</p> <p>Caution: This parameter is derived by the workflow. Under most circumstances, you should not change</p>

Additional Parameters Defined in this Step: Weblogic Domain Admin Server Validate Parameters, continued

Parameter Name	Default Value	Required	Description
			its mapping or its value.
Custom KeyStore PassPhrase	no default	optional	Password for the custom keystore.
Custom KeyStore Path	no default	optional	Fully qualified path to the custom keystore file.
Custom KeyStore Type	JKS	optional	The type of the Identity keystore.
Custom TrustStore PassPhrase	no default	optional	Password for the custom truststore.
Custom TrustStore Path	no default	optional	Fully qualified path to the custom truststore file.
Domain Path	no default	required	Fully qualified path where the domain and domain configuration will be created. For example: /opt/weblogic/user_projects/domains
Enable SSL	false	required	Tells the WebLogic 11g and 12c Administration Server to either use (true) or not use (false) the SSL port for communication.
Node Manager Port	5556	optional	Sets the port number under which the Node Manager will run.
Private Key Alias	no default	optional	The keystore attribute that defines the string alias used to store and retrieve the server's private key.
Setup Custom SSL Stores	no default	required	Determines whether you want to run Secure Socket Layer (SSL) with the demo SSL certificates or with your own custom keystore and truststore. Valid values are true or false. If Setup Custom SSL Stores is true, the following parameters must also be specified: Custom KeyStore PassPhrase, Custom KeyStore Path, Custom KeyStore Type, Custom TrustStore PassPhrase, Custom TrustStore Path, and Private Key Alias.
Start Node Manager	true	required	Determines whether to start the WebLogic 11g and 12c Node Manager. Valid values are true and false.
WLST Call Wrapper	no default	required	Command that will invoke the WebLogic Scripting Tool (WLST). For example: su <user> /opt/oracle/WebLogic/install/

Additional Parameters Defined in this Step: Weblogic Domain Admin Server Validate Parameters, continued

Parameter Name	Default Value	Required	Description
			<code>common/bin/wlst.sh</code> The fully qualified path will vary depending on where you installed the product. The <user> must have appropriate permissions.
Weblogic Admin Password	no default	required	The password that will be used to authenticate with the WebLogic 11g and 12c Administration Server.

WebLogic - Provision Advanced Domain and Admin Server

This workflow modifies an existing WebLogic 11g and 12c domain and Administration Server, enables the domain-wide administration port, configures logging attributes of the domain and Administration Server, and modifies the WebLogic Scripting Tool (WLST) script to enable connection through the WLST to the domain-wide administration port.

Benefits

This workflow has the following benefits:

- You need to have SSL configured before you run the workflow to enable the domain-wide administration port.
- The domain-wide administration port changes the behavior of the traffic between the Administration Server and the application servers.
- You can put the application servers into stand-by mode, allowing a hot swap.
- The workflow changes the WLST script to configure SSL communication to the domain-wide administration port.

To use this workflow in your environment, see the following information:

Topic	Information Included
"Prerequisites for this Workflow"	List of prerequisites that must be satisfied before you can run this workflow
"How this Workflow Works"	Information about what the workflow does, including validation checks performed, steps executed, and a high-level process flow
"How to Run this Workflow"	Instructions for running this workflow in your environment
"Sample Scenario"	Examples of typical parameter values for this workflow
Parameters	List of input parameters for this workflow.

Prerequisites for this Workflow

Be sure that the following prerequisites are satisfied before you run the ["WebLogic - Provision Advanced Domain and Admin Server"](#) workflow:

1. The latest DMA solution packs require the latest DMA platform. To use the latest solution packs, update the DMA platform. DMA10.50.001.000 solution packs are supported on DMA10.50.001.000 (and later).
2. You have installed the Application Server Provisioning Solution Pack.
3. The WebLogic 11g and 12c domain and Administration Server must exist and be configured to use SSL.

For more information about prerequisites for WebLogic 11g and 12c, refer to the [WebLogic Product Documentation](#).

How this Workflow Works

The following information describes how the ["WebLogic - Provision Advanced Domain and Admin Server"](#) workflow works:

Overview

The workflow does the following:

- Prepares to modify the WebLogic 11g and 12c domain and Administration Server advanced configurations by setting up the command to be used in subsequent steps, gathering and validating input parameters, and validating connection to the Administration Server.
- Uses the existing SSL keystore and truststore configurations and components that were previously created by the ["WebLogic - Create Trust and Identity Keystore" on page 1037](#).
- Modifies an existing WebLogic 11g and 12c domain and Administration Server—created by ["WebLogic - Provision Advanced Domain and Admin Server" on page 983](#)—to enable the domain-wide administration port and configure logging attributes.
- Modifies the WLST script to enable connection through WLST to the domain-wide administration port.
- Stops and restarts the WebLogic 11g and 12c Administration Server so that the changes take effect and then validates that the Administration Server came up successfully.

Validation Checks Performed

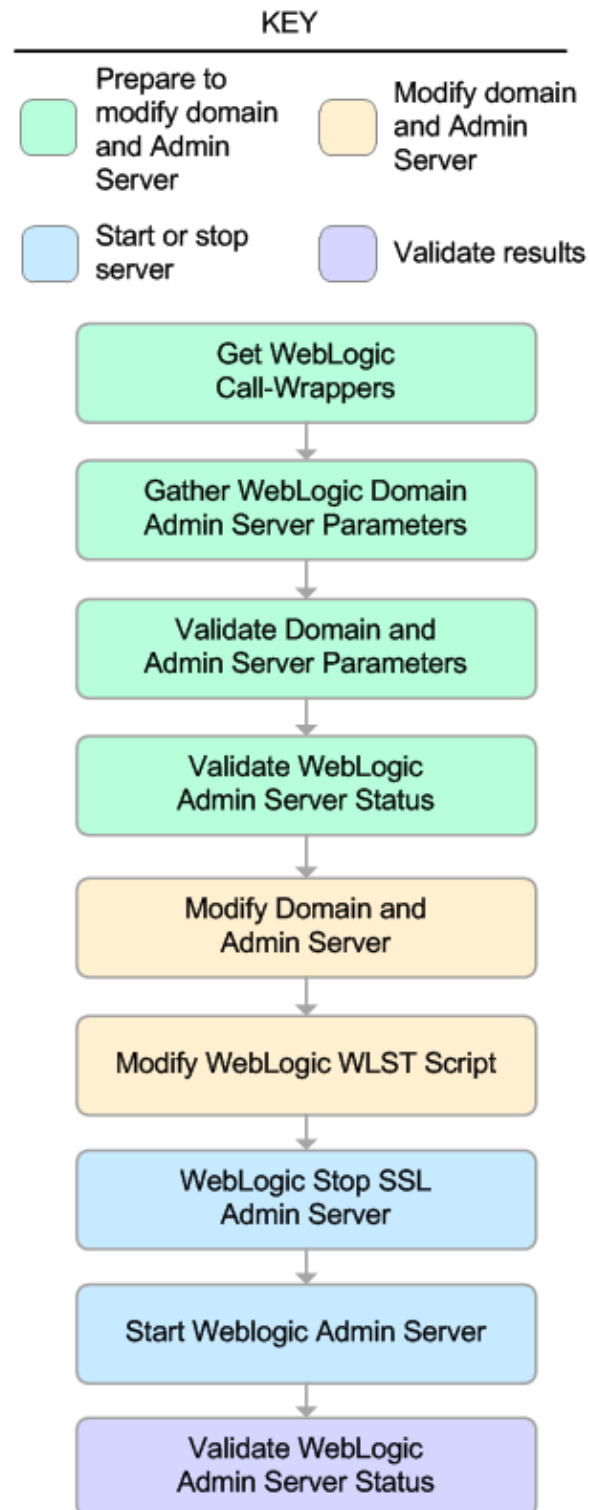
Much of the validation centers on the input parameters:

- Verifies that required parameters have values specified.
- Verifies that Admin Server Log Dir, Domain Path, Java Home,, and WLS Install Home are valid paths and exist.
- Verifies that TrustStore File Locations a valid existing path with a valid filename.
- Verifies that Admin Server Port, Admin SSL Port, and Domain Administration Port are valid integers.

The workflow also validates that the Administration Server is up and running before and after making the modifications.

Steps Executed

The WebLogic - Provision Advanced Domain and Admin Server workflow includes the following steps. Each step must complete successfully before the next step can start. If a step fails, the workflow reports a failure and all subsequent steps are skipped.



Steps Used in WebLogic - Provision Advanced Domain and Admin Server

Workflow Step	Description
Get WebLogic Call-Wrappers	This step creates the commands that subsequent steps will use to execute scripts and WebLogic 11g and 12c Scripting Tool (WLST) operations.
Gather WebLogic Domain Admin Server Parameters	This step gathers all required parameters to enable the domain-wide administration port, modify logging attributes, and modify the WLST script file.
Validate Domain and Admin Server Parameters	This step validates and prepares all required parameters to enable the domain-wide administration port, modify logging attributes, and modify the WLST script file.
Validate WebLogic Admin Server Status	This step validates that the Administration Server process is up and running.
Modify Domain and Admin Server	This step enables the domain-wide administration port and modifies logging attributes for the Administration Server.
Modify WebLogic WLST Script	This step modifies the WLST script file on the target machine to enable connections to the domain-wide administration port.
WebLogic Stop SSL Admin Server	This step stops the Administration SSL Server on a given machine or server.
Start Weblogic Admin Server	This step starts the WebLogic 11g and 12c Administration Server.
Validate WebLogic Admin Server Status	This step validates that the Administration Server process is up and running.

For parameter descriptions and defaults, see ["Parameters for WebLogic - Provision Advanced Domain and Admin Server"](#).

How to Run this Workflow

The following instructions show you how to customize and run the ["WebLogic - Provision Advanced Domain and Admin Server"](#) workflow in your environment.

Note: Before following this procedure, review the ["Prerequisites for this Workflow"](#) on page 984, and ensure that all requirements are satisfied.

To use the WebLogic - Provision Weblogic Domain and Admin Server workflow:

1. Create a deployable copy of the workflow.
2. Determine the values that you will specify for the following parameters:

Input Parameters for Get WebLogic Call-Wrappers

Parameter Name	Default Value	Required	Description
BEA Home	no default	required	Fully qualified path to the middleware home directory that contains the WebLogic 11g and 12c installation. For example: /opt/oracle/weblogic
WLS Install Home	no default	required	Fully qualified path to the directory where WebLogic Server will be installed. For example: /opt/oracle/weblogic/wlserver12.1

Input Parameters for Gather WebLogic Domain Admin Server Parameters

Parameter Name	Default Value	Required	Description
Admin SSL Port	no default	required	The Secure Sockets Layer (SSL) port on which the WebLogic 11g and 12c Administration Server will run. If Enable SSL is set to true, this parameter must also have a value.
Admin Server Hostname	Server.name	required	The WebLogic 11g and 12c Administration Server host name or IP address that the Administration Server will run on. The Administration Server is used to issue administrative commands to the Application Servers.
Admin Server Log Dir	no default	required	Log file directory location where the Administration Server logs will be written.
Admin Server Name	no default	required	Label or name given to the Administration Server.
Admin Server Port	no default	required	The non-SSL port on which the WebLogic 11g and 12c Administration Server will

Input Parameters for Gather WebLogic Domain Admin Server Parameters, continued

Parameter Name	Default Value	Required	Description
			run.
Domain Administration Port	no default	required	The common secure administration port for this WebLogic 11g and 12c Server domain.
Domain Name	no default	required	Name of the WebLogic 11g and 12c Server domain.
Domain Path	no default	required	Fully qualified path where the domain and domain configuration will be created. For example: /opt/weblogic/user_projects/domains
Java Home	no default	required	Fully qualified path to the JAVA_HOME that the WebLogic 11g and 12c domain uses. For example: /opt/oracle/jdk1.6.0_35
TrustStore File Location	no default	required	Fully qualified file path where the java truststore already exists. For example: /opt/app/ssl/mytruststore.jks
Weblogic Admin Password	no default	required	The password that will be used to authenticate with the WebLogic 11g and 12c Administration Server.
WebLogic Admin User	no default	required	The WebLogic 11g and 12c administrator account that will be used to authenticate with the Administration Server.

Note: See ["Parameters for WebLogic - Provision Advanced Domain and Admin Server"](#) for detailed descriptions of all input parameters for this workflow, including default values.

- In the workflow editor, expose any additional parameters that you need. You will specify values for those parameters when you create the deployment.
- Save the changes to the workflow (click **Save** in the lower right corner).
- Create a new deployment.
- On the Parameters tab, specify values for the required parameters listed in step 2 and any additional parameters that you have exposed. You do not need to specify values for those parameters whose default values are appropriate for your environment.
- On the Targets tab, specify one or more targets for this deployment.

Note: The target for this deployment should be set to the server where the WebLogic 11g and 12c Administration Server will be provisioned.

8. Save the deployment (click **Save** in the lower right corner).
9. Run the workflow using this deployment.

To verify the results:

The workflow will complete and report SUCCESS on the Console if it has run successfully. If an error occurs during the workflow execution, the error will be logged, and the workflow terminates in the FAILURE state.

Optional: If you want to further verify the results:

The workflow was successful if the Administration Server restarted successfully.

Sample Scenario

It is very straightforward to run the ["WebLogic - Provision Advanced Domain and Admin Server"](#) workflow. This topic shows you typical parameter values to use.

Typical parameters

Input Parameters for Get WebLogic Call-Wrappers

Parameter Name	Example Value	Description
BEA Home	see description	Fully qualified path to the middleware home directory that contains the WebLogic 11g and 12c installation. For example: /opt/oracle/weblogic
WLS Install Home	see description	Fully qualified path to the directory where WebLogic Server will be installed. For example: /opt/oracle/weblogic/wlserver12.1

Input Parameters for Gather WebLogic Domain Admin Server Parameters

Parameter Name	Example Value	Description
Admin SSL Port	no default	The Secure Sockets Layer (SSL) port on which the WebLogic Administration Server will run. If Enable SSL is set to true, this parameter must also have a value.
Admin Server Log Dir	Server.name	The WebLogic Administration Server host name or IP address that the Administration Server will run on. The Administration Server is used to issue administrative commands to the Application Servers.
Admin Server Name	no default	Log file directory location where the Administration Server logs will be written.
Admin Server Port	8001	The non-SSL port on which the WebLogic 11g and 12c Administration Server will run.
Domain Administration Port	5555	The common secure administration port for this WebLogic 11g and 12c Server domain.
Domain Name	MyDomain	Name of the WebLogic 11g and 12c Server domain.
Domain Path	see description	Fully qualified path where the domain and domain configuration will be created. For example: /opt/weblogic/user_projects/domains
Java Home	see description	Fully qualified path to the JAVA_HOME that the WebLogic 11g and 12c domain uses. For example: /opt/oracle/jdk1.6.0_35
TrustStore File Location	see description	Fully qualified file path where the java truststore already exists. For example: /opt/app/ssl/mytruststore.jks

Input Parameters for Gather WebLogic Domain Admin Server Parameters, continued

Parameter Name	Example Value	Description
Weblogic Admin Password	password	The password that will be used to authenticate with the WebLogic 11g and 12c Administration Server.
WebLogic Admin User	weblogic	The WebLogic 11g and 12c administrator account that will be used to authenticate with the Administration Server.

Parameters for WebLogic - Provision Advanced Domain and Admin Server

The following tables describe the required and optional input parameters for this workflow. Some of these parameters may not be initially visible in a deployment. For some parameters, if you do not specify a value for a parameter, a default value is assigned.

Following are tables for each of the steps used by this workflow where parameters are defined:

Parameters Defined in this Step: Get WebLogic Call-Wrappers

Parameter Name	Default Value	Required	Description
BEA Home	no default	required	Fully qualified path to the middleware home directory that contains the WebLogic 11g and 12c installation. For example: <code>/opt/oracle/weblogic</code>
WLS Install Home	no default	required	Fully qualified path to the directory where WebLogic Server will be installed. For example: <code>/opt/oracle/weblogic/wlserver12.1</code>

Additional Parameters Defined in this Step: Gather WebLogic Domain Admin Server Parameters

Parameter Name	Default Value	Required	Description
Admin SSL Port	no default	required	The Secure Sockets Layer (SSL) port on which the WebLogic 11g and 12c Administration Server will run. If Enable SSL is set to true, this parameter must also have a value.
Admin Server Hostname	Server.name	required	The WebLogic 11g and 12c Administration Server host name or IP address that the Administration Server will run on. The Administration Server is used to issue administrative commands to the Application Servers.
Admin Server Log Dir	no default	required	Log file directory location where the Administration Server logs will be written.
Admin Server Name	no default	required	Label or name given to the Administration Server.
Admin Server Port	no default	required	The non-SSL port on which the WebLogic 11g and 12c Administration Server will run.
Domain Administration Port	no default	required	The common secure administration port for this WebLogic 11g and 12c Server domain.
Domain Name	no default	required	Name of the WebLogic 11g and 12c Server domain.
Domain Path	no default	required	Fully qualified path where the domain and domain configuration will be created. For example:

Additional Parameters Defined in this Step: Gather WebLogic Domain Admin Server Parameters, continued

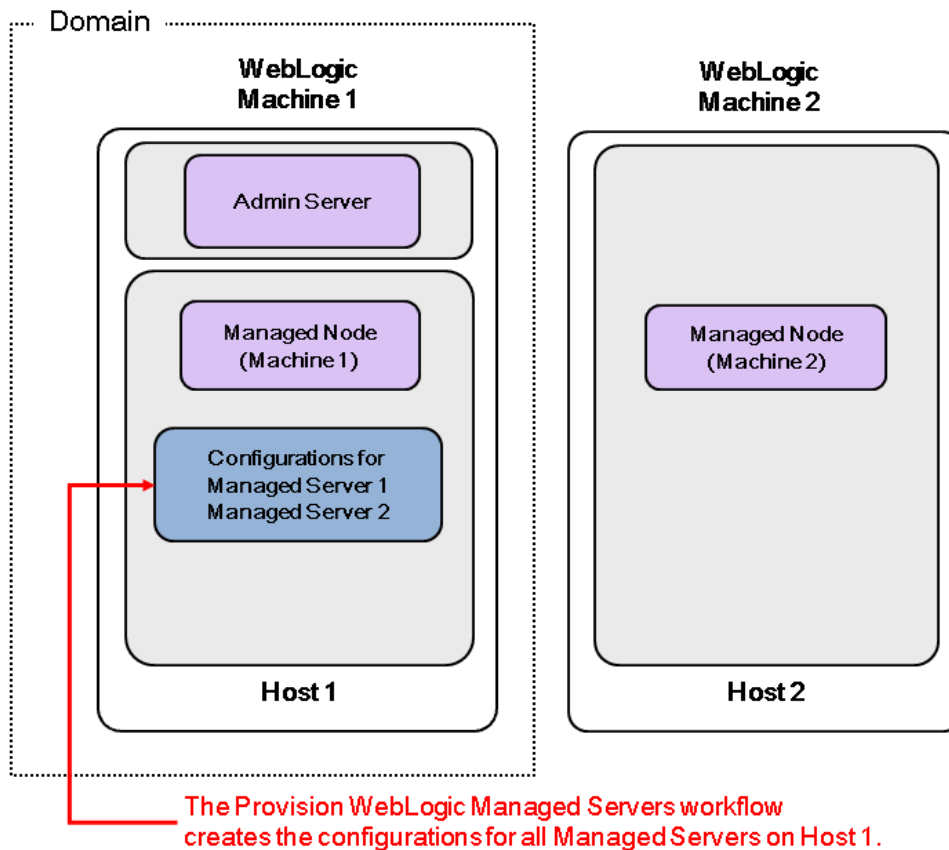
Parameter Name	Default Value	Required	Description
			/opt/weblogic/user_projects/domains
Java Home	no default	required	Fully qualified path to the JAVA_HOME that the WebLogic 11g and 12c domain uses. For example: /opt/oracle/jdk1.6.0_35
TrustStore File Location	no default	required	Fully qualified file path where the java truststore already exists. For example: /opt/app/ssl/mytruststore.jks
Weblogic Admin Password	no default	required	The password that will be used to authenticate with the WebLogic 11g and 12c Administration Server.
WebLogic Admin User	no default	required	The WebLogic 11g and 12c administrator account that will be used to authenticate with the Administration Server.

WebLogic - Provision Weblogic Managed Servers

This workflow creates a configuration for a WebLogic 11g and 12c Managed Server (or servers) from an existing installation and domain of WebLogic 11g and 12c.

You can group application servers together to optimize availability and scalability, or to manage your workload.

The following reference architecture diagram gives an example of what this workflow does:



To use this workflow in your environment, see the following information:

Topic	Information Included
"Prerequisites for this Workflow"	List of prerequisites that must be satisfied before you can run this workflow
"How this Workflow Works"	Information about what the workflow does, including validation checks performed, steps executed, and a high-level process flow
"How to Run this Workflow"	Instructions for running this workflow in your environment
"Sample Scenario"	Examples of typical parameter values for this workflow
Parameters	List of input parameters for this workflow.

Note: The documentation for this workflow contains steps that are referred to by their base names. The names in the DMA user interface may have a version appended, for example, v2.

Prerequisites for this Workflow

Be sure that the following prerequisites are satisfied before you run the ["WebLogic - Provision Weblogic Managed Servers"](#) workflow:

1. The latest DMA solution packs require the latest DMA platform. To use the latest solution packs, update the DMA platform. DMA10.50.001.000 solution packs are supported on DMA10.50.001.000 (and later).
2. You have installed the Application Server Provisioning Solution Pack.

For more information about prerequisites for WebLogic 11g and 12c, refer to the [WebLogic Product Documentation](#).

How this Workflow Works

The following information describes how the ["WebLogic - Provision Weblogic Managed Servers"](#) workflow works:

Overview

The workflow does the following:

- Prepares to provision the WebLogic 11g and 12c Managed Servers by setting up the command to be used in subsequent steps and validating input parameters.
- Creates the configurations for the Managed Servers using the WebLogic Scripting Tool (WLST). To do this, the workflow accesses the domain information, creates the servers, and then updates the domain.
- Stops and restarts the WebLogic 11g and 12c Administration Server and then starts any Managed Servers.

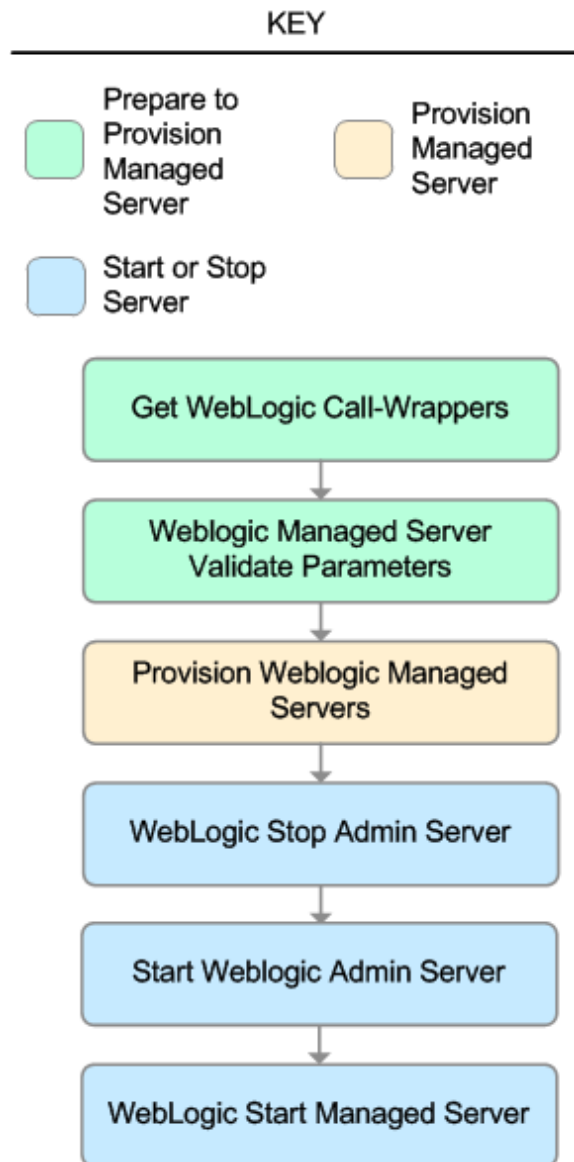
Validation Checks Performed

Much of the validation centers on the input parameters:

- Verifies that required parameters have values specified.
- Checks that the BEA Home and WLS Install Home files exist.
- Verifies that Enable Managed Server SSL, Setup Server Custom SSL, and Start Managed Servers are either true or false.
- If Setup Server Custom SSL is true, then Custom KeyStore PassPhrase, Custom KeyStore Path, Custom TrustStore PassPhrase, Custom TrustStore Path, and Private Key Alias are specified.
- Verifies that Managed Server Ports, Managed Server SSL Ports, and Managed Server Admin Ports are null or valid integers.
- Verifies that the lists are the same length for Managed Server Hostnames, Managed Server Names, Managed Server Ports, and Managed Server SSL Ports.

Steps Executed

The WebLogic - Provision Weblogic Managed Servers workflow includes the following steps. Each step must complete successfully before the next step can start. If a step fails, the workflow reports a failure and all subsequent steps are skipped.



Steps Used in WebLogic - Provision Weblogic Managed Servers

Workflow Step	Description
Get WebLogic Call-Wrappers	This step creates the commands that subsequent steps will use to execute scripts and WebLogic 11g and 12c Scripting Tool (WLST) operations.
Weblogic Managed Server Validate Parameters	This step prepares the parameters needed to create a Managed Server in WebLogic 11g and 12c.
Provision Weblogic Managed Servers	This step creates Managed Servers from an existing domain in WebLogic 11g and 12c. Optionally, the step enables SSL for the Managed Servers and configures the SSL port to listen. Optionally, the step configures the custom keystore and truststore. Optionally, if the "WebLogic - Provision Advanced Domain and Admin Server" on page 983 was run before this workflow, the step sets up the optional Domain Administration Port.
WebLogic Stop Admin Server	This step checks if the WebLogic 11g and 12c Administration Server on a given machine or server is running. If it is running, the step stops it.
Start Weblogic Admin Server	This step starts the WebLogic 11g and 12c Administration Server.
WebLogic Start Managed Server	This step connects to WebLogic 11g and 12c via WebLogic 11g and 12c Scripting Tool (WLST) and optionally starts all Managed Servers on a given machine or server.

For parameter descriptions and defaults, see ["Parameters for WebLogic - Provision Weblogic Managed Servers"](#).

How to Run this Workflow

The following instructions show you how to customize and run the ["WebLogic - Provision Weblogic Managed Servers"](#) workflow in your environment.

The workflow provides default values for some parameters. These default values are usually sufficient for a "typical" installation. You can override the defaults by specifying parameter values in the deployment. You can also expose additional parameters in the workflow, if necessary, to accomplish more advanced scenarios. Any parameters not explicitly specified in the deployment will have the default values listed in ["Parameters for WebLogic - Provision Weblogic Managed Servers"](#).

Note: Before following this procedure, review the ["Prerequisites for this Workflow"](#) on page 998, and ensure that all requirements are satisfied.

To use the WebLogic - Provision Weblogic Managed Servers workflow:

1. Create a deployable copy of the workflow.
2. Determine the values that you will specify for the following parameters:

Input Parameters for Get WebLogic Call-Wrappers

Parameter Name	Default Value	Required	Description
BEA Home	no default	required	Fully qualified path to the middleware home directory that contains the WebLogic 11g and 12c installation. For example: <code>/opt/oracle/weblogic</code>
WLS Install Home	no default	required	Fully qualified path to the directory where WebLogic Server will be installed. For example: <code>/opt/oracle/weblogic/wlserver12.1</code>

Input Parameters for Weblogic Managed Server Validate Parameters

Parameter Name	Default Value	Required	Description
Admin Server Name	no default	required	Label or name given to the Administration Server.
Admin Server Port	no default	required	The non-SSL port on which the WebLogic 11g and 12c Administration Server will run.
Custom KeyStore PassPhrase	no default	optional	Password for the custom keystore.
Custom KeyStore Path	no default	optional	Fully qualified path to the custom keystore file.

Input Parameters for Weblogic Managed Server Validate Parameters, continued

Parameter Name	Default Value	Required	Description
Custom TrustStore PassPhrase	no default	optional	Password for the custom truststore.
Custom TrustStore Path	no default	optional	Fully qualified path to the custom truststore file.
Domain Administration Port	no default	required	The common secure administration port for this WebLogic 11g and 12c Server domain.
Domain Path	no default	required	Fully qualified path where the domain and domain configuration will be created. For example: /opt/weblogic/user_projects/domains
Enable Managed Server SSL	no default	required	This parameter determines whether the Managed Server will use or not use the Secure Sockets Layer (SSL) port for communication. Valid values are true or false.
Managed Server Admin Ports	no default	required	The common secure domain-wide administration port that the Administration Server and Managed Server will communicate on.
Managed Server Hostnames	no default	required	Comma-delimited list of host names or IP addresses where each Managed Server will be provisioned. Note: The order of the host names or IP addresses specified must match the order specified in the following parameters: Managed Server Names, Managed Server Ports, and Managed Server SSL Ports.
Managed Server Names	no default	required	Comma-delimited list of the names of the Managed Servers to be provisioned. For example: Appserver1, Appserver2, Appserver3. Note: The order of the server names specified must match the order specified in the following parameters: Managed Server Hostnames, Managed Server Ports, and Managed Server SSL Ports.
Managed Server Ports	no default	required	Comma-delimited list of the ports on which the Managed Servers will listen. Note: The order of the ports specified must match the order specified in the following parameters: Managed Server Hostnames, Managed Server Names, and Managed Server SSL Ports.

Input Parameters for Weblogic Managed Server Validate Parameters, continued

Parameter Name	Default Value	Required	Description
Managed Server SSL Ports	no default	optional	Comma-delimited list of SSL ports on which the Managed Servers will listen. Note: The order of the SSL ports specified must match the order specified in the following parameters: Managed Server Hostnames, Managed Server Names, and Managed Server Ports.
Private Key Alias	no default	optional	The keystore attribute that defines the string alias used to store and retrieve the server's private key.
Setup Server Custom SSL Stores	no default	required	Determines whether you want to run Secure Socket Layer (SSL) with the demo SSL certificates or with your own custom keystore and truststore. Valid values are true or false. If Setup Server Custom SSL Stores is true, the following parameters must also be specified: Custom KeyStore Path, Custom KeyStore PassPhrase, Custom TrustStore Path, Custom TrustStore PassPhrase, and Private Key Alias.
Start Managed Servers	true	optional	Specifies whether or not to start up the managed servers once they have been created. Valid values are true and false.
WebLogic User Id	no default	required	The WebLogic 11g and 12c user that will be used to authenticate with the Administration Server.
WebLogic User Password	no default	required	The WebLogic 11g and 12c password that will be used to authenticate with the Administration Server.

Tip: To avoid having to re-enter passwords whenever they change, you can create a policy to provide them to the workflow.

Note: This is the minimum set of parameters required to run this workflow. You may need to expose additional parameters depending on your provisioning objectives.

See ["Parameters for WebLogic - Provision Weblogic Managed Servers"](#) for detailed descriptions of all input parameters for this workflow, including default values.

3. In the workflow editor, expose any additional parameters that you need. You will specify values for those parameters when you create the deployment.
4. Save the changes to the workflow (click **Save** in the lower right corner).
5. Create a new deployment.

6. On the Parameters tab, specify values for the required parameters listed in step 2 and any additional parameters that you have exposed. You do not need to specify values for those parameters whose default values are appropriate for your environment.
7. On the Targets tab, specify one or more targets for this deployment.

Note: The target for this deployment should be set to the server where the WebLogic 11g and 12c Administration Server is provisioned.

8. Save the deployment (click **Save** in the lower right corner).
9. Run the workflow using this deployment.

To verify the results:

The workflow will complete and report SUCCESS on the Console if it has run successfully. If an error occurs during the workflow execution, the error will be logged, and the workflow terminates in the FAILURE state.

Optional: If you want to further verify the results:

1. View the {DomainPath}/servers/{ManagedServerName}/logs/{ManagedServerName}.log file.
This file is created when the Managed Server is started up.
2. Look for the following to verify that the Managed Server (or servers) started:
Server started in RUNNING mode.

Sample Scenario

This topic shows you typical parameter values for different use cases for the ["WebLogic - Provision Weblogic Managed Servers"](#) workflow.

Scenario 1: Creates three Managed Servers on three separate hosts without configuring or enabling SSL

Set Setup Custom SSL Stores to false. Do not provide values for the following parameters: Custom KeyStore Path, Custom KeyStore PassPhrase, Custom TrustStore Path, Custom TrustStore PassPhrase, and Private Key Alias.

This scenario creates the following configuration of Managed Servers:

Managed Server configuration

Managed Server Name	Managed Server Hostname	Managed Server Port
Appserver1	Host1	8001
Appserver2	Host2	8002
Appserver3	Host3	8003

Input Parameters for Get WebLogic Call-Wrappers

Parameter Name	Example Value	Description
BEA Home	see description	Fully qualified path to the middleware home directory that contains the WebLogic 11g and 12c installation. For example: /opt/oracle/weblogic
WLS Install Home	see description	Fully qualified path to the directory where WebLogic Server will be installed. For example: /opt/oracle/weblogic/wlserver12.1

Input Parameters for Weblogic Managed Server Validate Parameters

Parameter Name	Example Value	Description
Admin Server Name	myAdminServer	Label or name given to the Administration Server.
Admin Server Port	8005	The non-SSL port on which the WebLogic 11g and 12c Administration Server will run.
Custom KeyStore PassPhrase		Password for the custom keystore.
Custom KeyStore		Fully qualified path to the custom keystore file.

Input Parameters for Weblogic Managed Server Validate Parameters, continued

Parameter Name	Example Value	Description
Path		
Custom TrustStore PassPhrase		Password for the custom truststore.
Custom TrustStore Path		Fully qualified path to the custom truststore file.
Domain Administration Port	5555	The common secure administration port for this WebLogic 11g and 12c Server domain.
Domain Path	see description	Fully qualified path where the domain and domain configuration will be created. For example: /opt/weblogic/user_projects/domains
Enable Managed Server SSL	false	This parameter determines whether the Managed Server will use or not use the Secure Sockets Layer (SSL) port for communication. Valid values are true or false.
Managed Server Admin Ports	5556	The common secure domain-wide administration port that the Administration Server and Managed Server will communicate on.
Managed Server Hostnames	Host1, Host2, Host3	Comma-delimited list of host names or IP addresses where each Managed Server will be provisioned. Note: The order of the host names or IP addresses specified must match the order specified in the following parameters: Managed Server Names, Managed Server Ports, and Managed Server SSL Ports.
Managed Server Names	AppServer1, AppServer2, AppServer3	Comma-delimited list of the names of the Managed Servers to be provisioned. For example: Appserver1, Appserver2, Appserver3. Note: The order of the server names specified must match the order specified in the following parameters: Managed Server Hostnames, Managed Server Ports, and Managed Server SSL Ports.
Managed Server Ports	8001, 8002, 8003	Comma-delimited list of the ports on which the Managed Servers will listen. Note: The order of the ports specified must match the order specified in the following parameters: Managed Server Hostnames, Managed Server Names, and Managed Server SSL Ports.
Managed Server SSL Ports		Comma-delimited list of SSL ports on which the Managed Servers will listen.

Input Parameters for Weblogic Managed Server Validate Parameters, continued

Parameter Name	Example Value	Description
		<p>Note: The order of the SSL ports specified must match the order specified in the following parameters: Managed Server Hostnames, Managed Server Names, and Managed Server Ports.</p>
Setup Server Custom SSL Stores	false	<p>Determines whether you want to run Secure Socket Layer (SSL) with the demo SSL certificates or with your own custom keystore and truststore. Valid values are true or false.</p> <p>If Setup Server Custom SSL Stores is true, the following parameters must also be specified: Custom KeyStore Path, Custom KeyStore PassPhrase, Custom TrustStore Path, Custom TrustStore PassPhrase, and Private Key Alias.</p>
Start Managed Servers	true	Specifies whether or not to start up the managed servers once they have been created. Valid values are true and false.
WebLogic User Id	weblogic01	The WebLogic 11g and 12c user that will be used to authenticate with the Administration Server.
WebLogic User Password	weblogic01	The WebLogic 11g and 12c password that will be used to authenticate with the Administration Server.

Be sure that the default values for all remaining input parameters are appropriate for your environment (see ["Parameters for WebLogic - Provision Weblogic Managed Servers"](#)).

Scenario 2: Create four Managed Servers on two hosts and configure and enable SSL

Use this case to set up SSL to have the Node Manager communicate via SSL. Set Setup Custom SSL Stores to true. Also provide values for the following parameters: Custom KeyStore Path, Custom KeyStore PassPhrase, Custom TrustStore Path, Custom TrustStore PassPhrase, and Private Key Alias.

This scenario creates the following configuration of Managed Servers:

Managed Server configuration

Managed Server Name	Managed Server Hostname	Managed Server Port	Managed Server SSL Port
Appserver1	Host1	8001	8881
Appserver2	Host1	8002	8882
Appserver3	Host2	8001	8881
Appserver4	Host2	8002	8882

Input Parameters for Get WebLogic Call-Wrappers

Parameter Name	Example Value	Description
BEA Home	see description	Fully qualified path to the middleware home directory that contains the WebLogic 11g and 12c installation. For example: /opt/oracle/weblogic
WLS Install Home	see description	Fully qualified path to the directory where WebLogic Server will be installed. For example: /opt/oracle/weblogic/wlserver12.1

Input Parameters for Weblogic Managed Server Validate Parameters

Parameter Name	Example Value	Description
Admin Server Name	myAdminServer	Label or name given to the Administration Server.
Admin Server Port	8005	The non-SSL port on which the WebLogic 11g and 12c Administration Server will run.
Custom KeyStore PassPhrase	password	Password for the custom keystore.
Custom KeyStore Path	/opt/WebLogic/keystore	Fully qualified path to the custom keystore file.
Custom TrustStore PassPhrase	password	Password for the custom truststore.

Input Parameters for Weblogic Managed Server Validate Parameters, continued

Parameter Name	Example Value	Description
Custom TrustStore Path	/opt/WebLogic/truststore	Fully qualified path to the custom truststore file.
Domain Administration Port	5555	The common secure administration port for this WebLogic 11g and 12c Server domain.
Domain Path	see description	Fully qualified path where the domain and domain configuration will be created. For example: /opt/weblogic/user_projects/domains
Enable Managed Server SSL	true	This parameter determines whether the Managed Server will use or not use the Secure Sockets Layer (SSL) port for communication. Valid values are true or false.
Managed Server Admin Ports	5556	The common secure domain-wide administration port that the Administration Server and Managed Server will communicate on.
Managed Server Hostnames	Host1, Host2, Host1, Host2	Comma-delimited list of host names or IP addresses where each Managed Server will be provisioned. Note: The order of the host names or IP addresses specified must match the order specified in the following parameters: Managed Server Names, Managed Server Ports, and Managed Server SSL Ports.
Managed Server Names	Appserver1, Appserver2, Appserver3, Appserver4	Comma-delimited list of the names of the Managed Servers to be provisioned. For example: Appserver1, Appserver2, Appserver3. Note: The order of the server names specified must match the order specified in the following parameters: Managed Server Hostnames, Managed Server Ports, and Managed Server SSL Ports.
Managed Server Ports	8001, 8002, 8001, 8002	Comma-delimited list of the ports on which the Managed Servers will listen. Note: The order of the ports specified must match the order specified in the following parameters: Managed Server Hostnames, Managed Server Names, and Managed Server SSL Ports.
Managed Server SSL Ports	8881,8882,8881, 8882	Comma-delimited list of SSL ports on which the Managed Servers will listen. Note: The order of the SSL ports specified must match the order specified in the following parameters: Managed Server Hostnames, Managed Server Names, and Managed Server Ports.

Input Parameters for Weblogic Managed Server Validate Parameters, continued

Parameter Name	Example Value	Description
Private Key Alias	Hostname	The keystore attribute that defines the string alias used to store and retrieve the server's private key.
Setup Server Custom SSL Stores	true	<p>Determines whether you want to run Secure Socket Layer (SSL) with the demo SSL certificates or with your own custom keystore and truststore. Valid values are true or false.</p> <p>If Setup Server Custom SSL Stores is true, the following parameters must also be specified: Custom KeyStore Path, Custom KeyStore PassPhrase, Custom TrustStore Path, Custom TrustStore PassPhrase, and Private Key Alias.</p>
Start Managed Servers	true	Specifies whether or not to start up the managed servers once they have been created. Valid values are true and false.
WebLogic User Id	weblogic01	The WebLogic 11g and 12c user that will be used to authenticate with the Administration Server.
WebLogic User Password	weblogic01	The WebLogic 11g and 12c password that will be used to authenticate with the Administration Server.

Be sure that the default values for all remaining input parameters are appropriate for your environment (see ["Parameters for WebLogic - Provision Weblogic Managed Servers"](#)).

Parameters for WebLogic - Provision Weblogic Managed Servers

The following tables describe the required and optional input parameters for this workflow. Some of these parameters may not be initially visible in a deployment. For some parameters, if you do not specify a value for a parameter, a default value is assigned.

Following are tables for each of the steps used by this workflow where parameters are defined:

Parameters Defined in this Step: Get WebLogic Call-Wrappers

Parameter Name	Default Value	Required	Description
BEA Home	no default	required	Fully qualified path to the middleware home directory that contains the WebLogic 11g and 12c installation. For example: <code>/opt/oracle/weblogic</code>
WLS Install Home	no default	required	Fully qualified path to the directory where WebLogic Server will be installed. For example: <code>/opt/oracle/weblogic/wlserver12.1</code>

Additional Parameters Defined in this Step: Weblogic Managed Server Validate Parameters

Parameter Name	Default Value	Required	Description
Admin Server Hostname	Server.name	required	The WebLogic 11g and 12c Administration Server host name or IP address that the Administration Server will run on. The Administration Server is used to issue administrative commands to the Application Servers.
Admin Server Name	no default	required	Label or name given to the Administration Server.
Admin Server Port	no default	required	The non-SSL port on which the WebLogic 11g and 12c Administration Server will run.
Custom KeyStore PassPhrase	no default	optional	Password for the custom keystore.
Custom KeyStore Path	no default	optional	Fully qualified path to the custom keystore file.
Custom TrustStore PassPhrase	no default	optional	Password for the custom truststore.
Custom TrustStore Path	no default	optional	Fully qualified path to the custom truststore file.
Domain Administration	no default	required	The common secure administration port for this WebLogic 11g and 12c Server domain.

Additional Parameters Defined in this Step: Weblogic Managed Server Validate Parameters, continued

Parameter Name	Default Value	Required	Description
Port			
Domain Path	no default	required	Fully qualified path where the domain and domain configuration will be created. For example: /opt/weblogic/user_projects/domains
Enable Managed Server SSL	no default	required	This parameter determines whether the Managed Server will use or not use the Secure Sockets Layer (SSL) port for communication. Valid values are true or false.
Managed Server Admin Ports	no default	required	The common secure domain-wide administration port that the Administration Server and Managed Server will communicate on.
Managed Server Hostnames	no default	required	Comma-delimited list of host names or IP addresses where each Managed Server will be provisioned. Note: The order of the host names or IP addresses specified must match the order specified in the following parameters: Managed Server Names, Managed Server Ports, and Managed Server SSL Ports.
Managed Server Names	no default	required	Comma-delimited list of the names of the Managed Servers to be provisioned. For example: Appserver1, Appserver2, Appserver3. Note: The order of the server names specified must match the order specified in the following parameters: Managed Server Hostnames, Managed Server Ports, and Managed Server SSL Ports.
Managed Server Ports	no default	required	Comma-delimited list of the ports on which the Managed Servers will listen. Note: The order of the ports specified must match the order specified in the following parameters: Managed Server Hostnames, Managed Server Names, and Managed Server SSL Ports.
Managed Server SSL Ports	no default	optional	Comma-delimited list of SSL ports on which the Managed Servers will listen. Note: The order of the SSL ports specified must match the order specified in the following parameters: Managed Server Hostnames, Managed Server Names, and Managed Server Ports.
Private Key Alias	no default	optional	The keystore attribute that defines the string alias used to store and retrieve the server's private key.

Additional Parameters Defined in this Step: Weblogic Managed Server Validate Parameters, continued

Parameter Name	Default Value	Required	Description
Setup Server Custom SSL Stores	no default	required	<p>Determines whether you want to run Secure Socket Layer (SSL) with the demo SSL certificates or with your own custom keystore and truststore. Valid values are true or false.</p> <p>If Setup Server Custom SSL Stores is true, the following parameters must also be specified: Custom KeyStore Path, Custom KeyStore PassPhrase, Custom TrustStore Path, Custom TrustStore PassPhrase, and Private Key Alias.</p>
Start Managed Servers	true	optional	Specifies whether or not to start up the managed servers once they have been created. Valid values are true and false.
WLST Call Wrapper	no default	required	<p>Command that will invoke the WebLogic Scripting Tool (WLST). For example:</p> <pre>su <user> /opt/oracle/WebLogic/install/common/bin/wlst.sh</pre> <p>The fully qualified path will vary depending on where you installed the product. The <user> must have appropriate permissions.</p>
WebLogic User Id	no default	required	The WebLogic 11g and 12c user that will be used to authenticate with the Administration Server.
WebLogic User Password	no default	required	The WebLogic 11g and 12c password that will be used to authenticate with the Administration Server.

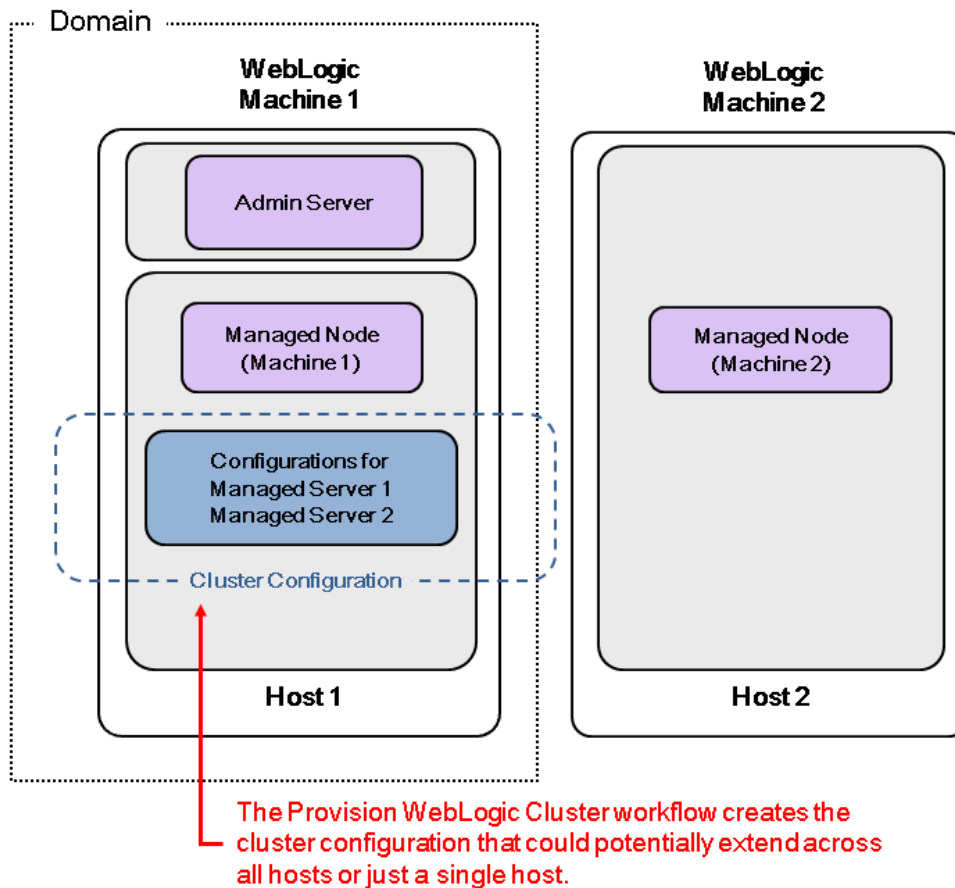
Provision WebLogic Cluster

This workflow creates a WebLogic 11g and 12c cluster configuration from an existing installation and domain of WebLogic 11g and 12c and adds the existing Managed Servers to the cluster configuration.

This workflow is optional. Use it only if you want to organize your Managed Servers into a cluster. Clusters allow your WebLogic 11g and 12c environment to be highly-available and load-balanced.

Your cluster can span the Managed Servers on a single machine (a vertical cluster) or across multiple machines (a horizontal cluster).

The following reference architecture diagram gives an example of what this workflow does:



Before you can run this workflow you need to have an operational WebLogic 11g or 12c environment.

Note: If you do not plan to expand the domain, you should manually start the cluster after running this workflow.

You can specify input parameters to select either multicast or unicast cluster messaging mode for your cluster.

To use this workflow in your environment, see the following information:

Topic	Information Included
"Prerequisites for this Workflow"	List of prerequisites that must be satisfied before you can run this workflow
"How this Workflow Works"	Information about what the workflow does, including validation checks performed, steps executed, and a high-level process flow
"How to Run this Workflow"	Instructions for running this workflow in your environment
"Sample Scenario"	Examples of typical parameter values for this workflow
Parameters	List of input parameters for this workflow.

Prerequisites for this Workflow

Be sure that the following prerequisites are satisfied before you run the ["Provision WebLogic Cluster"](#) workflow:

1. The latest DMA solution packs require the latest DMA platform. To use the latest solution packs, update the DMA platform. DMA10.50.001.000 solution packs are supported on DMA10.50.001.000 (and later).
2. You have installed the Application Server Provisioning Solution Pack.

For more information about prerequisites for WebLogic 11g and 12c, refer to the [WebLogic Product Documentation](#).

How this Workflow Works

The following information describes how the ["Provision WebLogic Cluster"](#) workflow works:

Overview

The workflow does the following:

- Prepares to provision the WebLogic 11g and 12c cluster by setting up the command to be used in subsequent steps and validating input parameters.
- Creates the cluster configuration using the WebLogic Scripting Tool (WLST): accesses the domain information, creates the cluster, sets the cluster messaging mode to either multicast or unicast, assigns the Managed Server (or servers) to the cluster, then updates the domain.
- Stops and restarts the WebLogic 11g and 12c Administration Server.

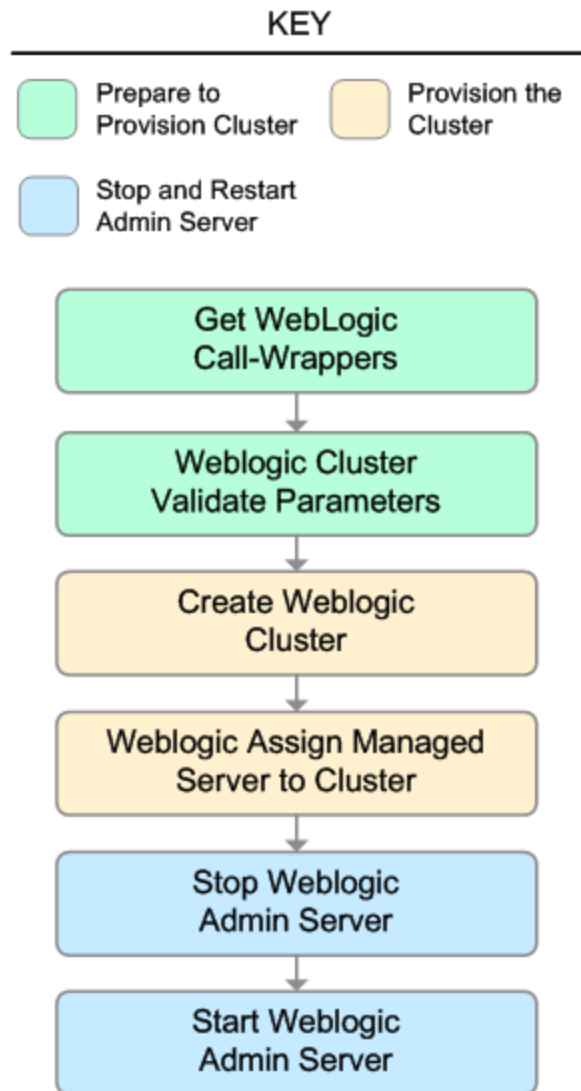
Validation Checks Performed

Much of the validation centers on the input parameters:

- Checks that the BEA Home and WLS Install Home files exist.
- Verifies that Multicast Port is null or a valid integer.
- If either Multicast Address or Multicast Port are null then the cluster messaging mode will be set to unicast. Otherwise it will be set to multicast.

Steps Executed

The Provision WebLogic Cluster workflow includes the following steps. Each step must complete successfully before the next step can start. If a step fails, the workflow reports a failure and all subsequent steps are skipped.



Steps Used in Provision WebLogic Cluster

Workflow Step	Description
Get WebLogic Call-Wrappers	This step creates the commands that subsequent steps will use to execute scripts and WebLogic 11g and 12c Scripting Tool (WLST) operations.
Weblogic Cluster Validate Parameters	This step prepares the parameters needed to create a cluster and add Managed Servers to the cluster on WebLogic 11g and 12c.
Create Weblogic Cluster	This step creates a cluster from an existing domain and installation of WebLogic 11g and 12c.
Weblogic Assign Managed Server to Cluster	This step adds Managed Servers to an existing cluster on WebLogic 11g and 12c.
WebLogic Stop Admin Server	This step checks if the WebLogic 11g and 12c Administration Server on a given machine or server is running. If it is running, the step stops it.
Start Weblogic Admin Server	This step starts the WebLogic 11g and 12c Administration Server.

For parameter descriptions and defaults, see ["Parameters for Provision WebLogic Cluster" on page 1025](#).

How to Run this Workflow

The following instructions show you how to customize and run the ["Provision WebLogic Cluster"](#) workflow in your environment.

The workflow provides default values for some parameters. These default values are usually sufficient for a "typical" installation. You can override the defaults by specifying parameter values in the deployment. You can also expose additional parameters in the workflow, if necessary, to accomplish more advanced scenarios. Any parameters not explicitly specified in the deployment will have the default values listed in ["Parameters for Provision WebLogic Cluster" on page 1025](#).

Note: Before following this procedure, review the ["Prerequisites for this Workflow" on page 1017](#), and ensure that all requirements are satisfied.

To use the Provision WebLogic Cluster workflow:

1. Create a deployable copy of the workflow.
2. Determine the values that you will specify for the following parameters:

Input Parameters for Get WebLogic Call-Wrappers

Parameter Name	Default Value	Required	Description
BEA Home	no default	required	Fully qualified path to the middleware home directory that contains the WebLogic 11g and 12c installation. For example: /opt/oracle/weblogic
WLS Install Home	no default	required	Fully qualified path to the directory where WebLogic Server will be installed. For example: /opt/oracle/weblogic/wlserver12.1

Input Parameters for Weblogic Cluster Validate Parameters

Parameter Name	Default Value	Required	Description
Cluster Name	no default	required	The name of the new cluster. For example: ClusterAppServer.
Domain Path	no default	required	Fully qualified path where the domain and domain configuration will be created. For example: /opt/weblogic/user_projects/domains
Managed Servers	no default	required	Comma-delimited list of the names of the Managed Server (or servers) that will be added to the new cluster. For example: AppServer1, AppServer2.
Multicast	no	required	The multicast address that will be used by cluster

Input Parameters for Weblogic Cluster Validate Parameters, continued

Parameter Name	Default Value	Required	Description
Address	default		members to communicate with each other. Specify this ONLY if you intend to use multicast for cluster communication.
Multicast Port	no default	required	The multicast port (between 1 and 65535) that will be used by cluster members to communicate with each other. Specify this ONLY if you intend to use multicast for cluster communication.

Note: See ["Parameters for Provision WebLogic Cluster" on page 1025](#) for detailed descriptions of all input parameters for this workflow, including default values.

3. In the workflow editor, expose any additional parameters that you need. You will specify values for those parameters when you create the deployment.
4. Save the changes to the workflow (click **Save** in the lower right corner).
5. Create a new deployment.
6. On the Parameters tab, specify values for the required parameters listed in step 2 and any additional parameters that you have exposed. You do not need to specify values for those parameters whose default values are appropriate for your environment.
7. On the Targets tab, specify one or more targets for this deployment.

Note: The target for this deployment should be set to the server where the WebLogic 11g and 12c Administration Server is provisioned.

8. Save the deployment (click **Save** in the lower right corner).
9. Run the workflow using this deployment.

Note: If you do not plan to expand the domain, you should manually start the cluster after running this workflow.

To verify the results:

The workflow will complete and report SUCCESS on the Console if it has run successfully. If an error occurs during the workflow execution, the error will be logged, and the workflow terminates in the FAILURE state.

Sample Scenario

This topic shows you typical parameter values for different use cases for the ["Provision WebLogic Cluster"](#) workflow.

Scenario 1: To use multicast

If you intend to use multicast for cluster communication, set both Multicast Address and Multicast Port to appropriate values.

Input Parameters for Get WebLogic Call-Wrappers

Parameter Name	Example Value	Description
BEA Home	no default	Fully qualified path to the middleware home directory that contains the WebLogic 11g and 12c installation. For example: /opt/oracle/weblogic
WLS Install Home	no default	Fully qualified path to the directory where WebLogic Server will be installed. For example: /opt/oracle/weblogic/wlserver12.1

Input Parameters for Weblogic Cluster Validate Parameters

Parameter Name	Example Value	Description
Cluster Name	see description	The name of the new cluster. For example: ClusterAppServer.
Domain Path	see description	Fully qualified path where the domain and domain configuration will be created. For example: /opt/weblogic/user_projects/domains
Managed Servers	see description	Comma-delimited list of the names of the Managed Server (or servers) that will be added to the new cluster. For example: AppServer1, AppServer2.
Multicast Address	237.0.0.101	The multicast address that will be used by cluster members to communicate with each other. Specify this ONLY if you intend to use multicast for cluster communication.
Multicast Port	9200	The multicast port (between 1 and 65535) that will be used by cluster members to communicate with each other. Specify this ONLY if you intend to use multicast for cluster communication.

Be sure that the default values for all remaining input parameters are appropriate for your environment (see ["Parameters for Provision WebLogic Cluster"](#) on page 1025).

Scenario 2: To use unicast

If you intend to use unicast for cluster communication, do not set either Multicast Address or Multicast Port .

Input Parameters for Get WebLogic Call-Wrappers

Parameter Name	Example Value	Description
BEA Home	no default	Fully qualified path to the middleware home directory that contains the WebLogic 11g and 12c installation. For example: /opt/oracle/weblogic
WLS Install Home	no default	Fully qualified path to the directory where WebLogic Server will be installed. For example: /opt/oracle/weblogic/wlserver12.1

Input Parameters for Weblogic Cluster Validate Parameters

Parameter Name	Example Value	Description
Cluster Name	see description	The name of the new cluster. For example: ClusterAppServer.
Domain Path	see description	Fully qualified path where the domain and domain configuration will be created. For example: /opt/weblogic/user_projects/domains
Managed Servers	see description	Comma-delimited list of the names of the Managed Server (or servers) that will be added to the new cluster. For example: AppServer1, AppServer2.
Multicast Address		The multicast address that will be used by cluster members to communicate with each other. Specify this ONLY if you intend to use multicast for cluster communication.
Multicast Port		The multicast port (between 1 and 65535) that will be used by cluster members to communicate with each other. Specify this ONLY if you intend to use multicast for cluster communication.

Be sure that the default values for all remaining input parameters are appropriate for your environment (see ["Parameters for Provision WebLogic Cluster" on the next page](#)).

Parameters for Provision WebLogic Cluster

The following tables describe the required and optional input parameters for this workflow. Some of these parameters may not be initially visible in a deployment. For some parameters, if you do not specify a value for a parameter, a default value is assigned.

Following are tables for each of the steps used by this workflow where parameters are defined:

Parameters Defined in this Step: Get WebLogic Call-Wrappers

Parameter Name	Default Value	Required	Description
BEA Home	no default	required	Fully qualified path to the middleware home directory that contains the WebLogic 11g and 12c installation. For example: <code>/opt/oracle/weblogic</code>
WLS Install Home	no default	required	Fully qualified path to the directory where WebLogic Server will be installed. For example: <code>/opt/oracle/weblogic/wlserver12.1</code>

Additional Parameters Defined in this Step: Weblogic Cluster Validate Parameters

Parameter Name	Default Value	Required	Description
Cluster Name	no default	required	The name of the new cluster. For example: ClusterAppServer.
Domain Path	no default	required	Fully qualified path where the domain and domain configuration will be created. For example: <code>/opt/weblogic/user_projects/domains</code>
Managed Servers	no default	required	Comma-delimited list of the names of the Managed Server (or servers) that will be added to the new cluster. For example: AppServer1, AppServer2.
Multicast Address	no default	optional	The multicast address that will be used by cluster members to communicate with each other. Specify this ONLY if you intend to use multicast for cluster communication.
Multicast Port	no default	optional	The multicast port (between 1 and 65535) that will be used by cluster members to communicate with each other. Specify this ONLY if you intend to use multicast for cluster communication.
WLST Call Wrapper	no default	required	Command that will invoke the WebLogic Scripting Tool (WLST). For example: <code>su <user> /opt/oracle/WebLogic/install/common/bin/wlst.sh</code> The fully qualified path will vary depending on where you installed the product. The <user> must have appropriate permissions.

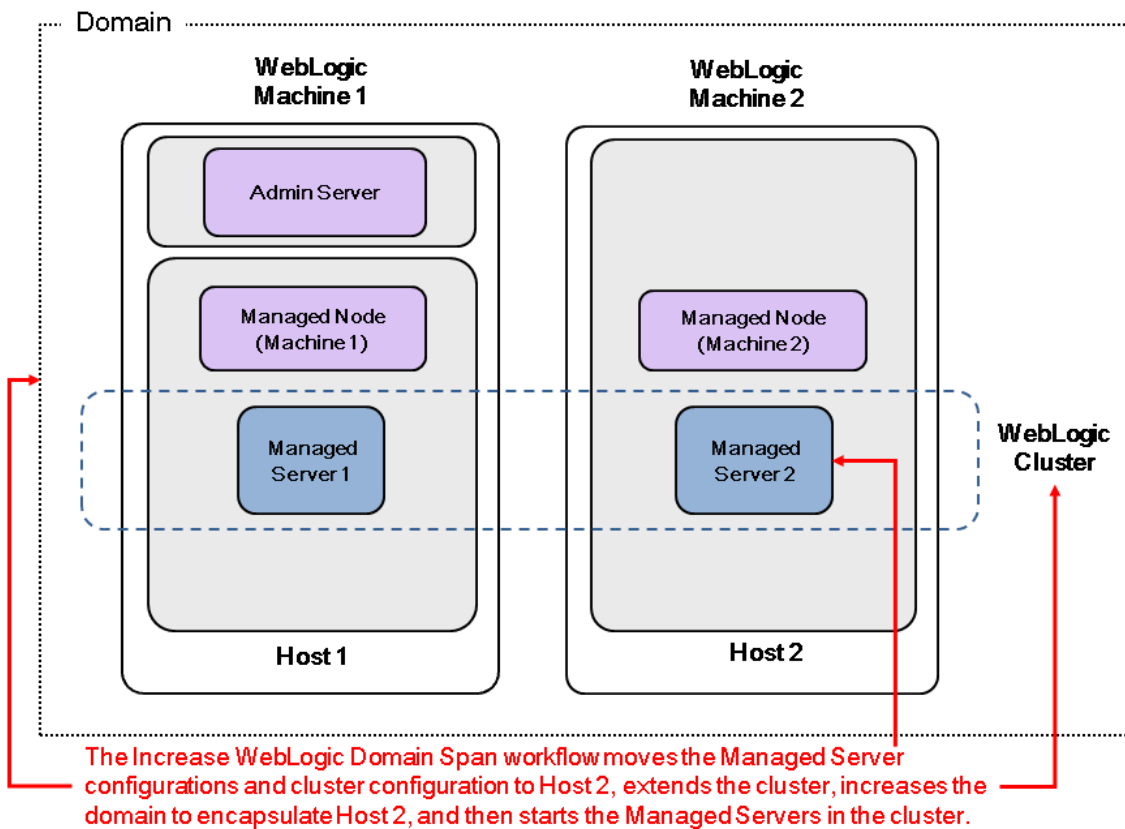
Increase WebLogic Domain Span

This workflow increases the span of a WebLogic 11g and 12c domain by adding other hosts to that domain. To accomplish this it moves the Managed Server configurations and cluster configuration to the other hosts, extends the cluster, starts the Managed Servers, and starts the cluster.

The basic process is to pack up the domain into a template file, send that file to the remote machines, and then unpack it into the correct locations.

This workflow is optional. Use it only if your domain spans more than one machine.

The following reference architecture diagram gives an example of what this workflow does:



Before you can run this workflow you need to have an operational WebLogic 11g or 12c with a horizontal cluster.

Note: Before running this workflow set up the SSH keys between the original domain's machine and the target machine (or machines).

To use this workflow in your environment, see the following information:

Topic	Information Included
"Prerequisites for this Workflow"	List of prerequisites that must be satisfied before you can run this workflow
"How this Workflow Works"	Information about what the workflow does, including validation checks performed, steps executed, and a high-level process flow
"How to Run this Workflow"	Instructions for running this workflow in your environment
"Sample Scenario"	Examples of typical parameter values for this workflow
Parameters	List of input parameters for this workflow.

Prerequisites for this Workflow

Be sure that the following prerequisites are satisfied before you run the ["Increase WebLogic Domain Span"](#) workflow:

1. The latest DMA solution packs require the latest DMA platform. To use the latest solution packs, update the DMA platform. DMA 10.30 solution packs are supported on DMA 10.30 (and later).
2. You have installed the Application Server Provisioning Solution Pack.
3. SSH keys are set up between the original domain's machine and the target machine (or machines). These shared keys set up Trust IDs to log in without a password.

For more information about prerequisites for WebLogic 11g and 12c, refer to the [WebLogic Product Documentation](#).

How this Workflow Works

The following information describes how the ["Increase WebLogic Domain Span"](#) workflow works:

Overview

The workflow does the following:

- Sets up the command to be used to increase the WebLogic 11g and 12c domain span.
- Uses the pack utility to pack up the domain into a template file, sends that file to the remote machine (or machines), then uses the unpack utility to unpack it into the correct location.

In more detail, this workflow uses the internal tool in WebLogic 11g and 12c to jar up the configurations for the Managed Servers and the cluster configuration into an archive file. Then it pushes via Secure Copy (SCP) and moves the JAR file to the other machines. Finally, it uses the same utility to unjar the archive file onto the other machines.

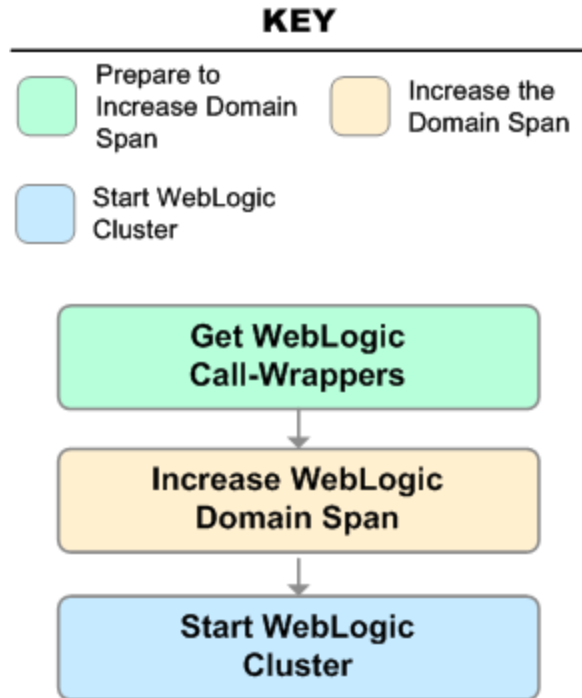
- Starts up the cluster in the WebLogic 11g and 12c domain.

Validation Checks Performed

This workflow checks that the BEA Home and WLS Install Home files exist.

Steps Executed

The "Increase WebLogic Domain Span" workflow includes the following steps. Each step must complete successfully before the next step can start. If a step fails, the workflow reports a failure and all subsequent steps are skipped.



Steps Used in Increase WebLogic Domain Span

Workflow Step	Description
Get WebLogic Call-Wrappers	This step creates the commands that subsequent steps will use to execute scripts and WebLogic 11g and 12c Scripting Tool (WLST) operations.
Increase WebLogic Domain Span	This step uses the pack and unpack utilities within the WebLogic 11g and 12c product to pack up the domain configuration and unpack it on a remote target machine (or machines).
Start WebLogic Cluster	This step starts up the cluster in the WebLogic 11g and 12c domain.

For parameter descriptions and defaults, see ["Parameters for Increase WebLogic Domain Span" on page 1035](#).

How to Run this Workflow

The following instructions show you how to customize and run the ["Increase WebLogic Domain Span"](#) workflow in your environment.

The workflow provides default values for some parameters. These default values are usually sufficient for a "typical" installation. You can override the defaults by specifying parameter values in the deployment. You can also expose additional parameters in the workflow, if necessary, to accomplish more advanced scenarios. Any parameters not explicitly specified in the deployment will have the default values listed in ["Parameters for Increase WebLogic Domain Span" on page 1035](#).

Note: Before following this procedure, review the ["Prerequisites for this Workflow" on page 1028](#), and ensure that all requirements are satisfied.

To use the Increase WebLogic Domain Span workflow:

1. Create a deployable copy of the workflow.
2. Determine the values that you will specify for the following parameters:

Input Parameters for Get WebLogic Call-Wrappers

Parameter Name	Default Value	Required	Description
BEA Home	no default	required	Fully qualified path to the middleware home directory that contains the WebLogic 11g and 12c installation. For example: /opt/oracle/weblogic
WLS Install Home	no default	required	Fully qualified path to the directory where WebLogic Server will be installed. For example: /opt/oracle/weblogic/wlserver12.1

Input Parameters for Increase WebLogic Domain Span

Parameter Name	Default Value	Required	Description
Local Domain Path	no default	required	Path to the local domain. If the specified path is a relative path, it is assumed to be relative to BEA Home. For example: /opt/oracle/weblogic/user_projects/domains/base_domain where /opt/oracle/weblogic is the BEA Home.
Local Template Path	no default	required	Path to the local template directory or the path to a template file. If the specified path is a relative path, it is assumed to be relative to BEA Home. For example: /opt/oracle/weblogic/user_projects/domains/base_

Input Parameters for Increase WebLogic Domain Span, continued

Parameter Name	Default Value	Required	Description
			domain.jar where /opt/oracle/weblogic is the BEA Home.
Remote Addresses	no default	required	Comma-delimited list of hosts (DNS addresses or IP addresses) that the domain will span.

Input Parameters for Start WebLogic Cluster

Parameter Name	Default Value	Required	Description
Admin Server Port	no default	optional	The non-SSL port on which the WebLogic 11g and 12c Administration Server will run.
Cluster Name	no default	required	The name of the new cluster. For example: ClusterAppServer.
Weblogic Admin Password	no default	required	The password that will be used to authenticate with the WebLogic 11g and 12c Administration Server.
WebLogic Admin User	weblogic	required	The WebLogic 11g and 12c administrator account that will be used to authenticate with the Administration Server.

Note: This is the minimum set of parameters required to run this workflow. You may need to expose additional parameters depending on your objectives.

See ["Parameters for Increase WebLogic Domain Span" on page 1035](#) for detailed descriptions of all input parameters for this workflow, including default values.

3. In the workflow editor, expose any additional parameters that you need. You will specify values for those parameters when you create the deployment.
4. Save the changes to the workflow (click **Save** in the lower right corner).
5. Create a new deployment.
6. On the Parameters tab, specify values for the required parameters listed in step 2 and any additional parameters that you have exposed. You do not need to specify values for those parameters whose default values are appropriate for your environment.
7. On the Targets tab, specify one or more targets for this deployment.

Note: The target for this deployment should be set to the server where the WebLogic 11g and 12c Administration Server is provisioned.

The workflow pushes the configuration over to other hosts based on your input parameters.

8. Save the deployment (click **Save** in the lower right corner).
9. Run the workflow using this deployment.

To verify the results:

The workflow will complete and report SUCCESS on the Console if it has run successfully. If an error occurs during the workflow execution, the error will be logged, and the workflow terminates in the FAILURE state.

Optional: If you want to further verify the results:

1. View the `{BEAHOME}/logs/log.txt` file.
This file is created after the installation is complete.
2. Look for specific information about what was installed.

Sample Scenario

It is very straightforward to run the ["Increase WebLogic Domain Span"](#) workflow. This topic shows you typical parameter values to use.

Typical parameters:

Input Parameters for Get WebLogic Call-Wrappers

Parameter Name	Example Value	Description
BEA Home	see description	Fully qualified path to the middleware home directory that contains the WebLogic 11g and 12c installation. For example: /opt/oracle/weblogic
WLS Install Home	see description	Fully qualified path to the directory where WebLogic Server will be installed. For example: /opt/oracle/weblogic/wlserver12.1

Input Parameters for Increase WebLogic Domain Span

Parameter Name	Example Value	Description
Local Domain Path	see description	Path to the local domain. If the specified path is a relative path, it is assumed to be relative to BEA Home. For example: /opt/oracle/weblogic/user_projects/domains/base_domain where /opt/oracle/weblogic is the BEA Home.
Local Template Path	see description	Path to the local template directory or the path to a template file. If the specified path is a relative path, it is assumed to be relative to BEA Home. For example: /opt/oracle/weblogic/user_projects/domains/base_domain.jar where /opt/oracle/weblogic is the BEA Home.
Remote Addresses	server. company.com	Comma-delimited list of hosts (DNS addresses or IP addresses) that the domain will span.

Input Parameters for Start WebLogic Cluster

Parameter Name	Example Value	Description
Admin Server Port	8001	The non-SSL port on which the WebLogic 11g and 12c Administration Server will run.
Cluster Name	see description	The name of the new cluster. For example: ClusterAppServer.

Be sure that the default values for all remaining input parameters are appropriate for your environment (see ["Parameters for Increase WebLogic Domain Span" on the next page](#)).

Parameters for Increase WebLogic Domain Span

The following tables describe the required and optional input parameters for this workflow. Some of these parameters may not be initially visible in a deployment. For some parameters, if you do not specify a value for a parameter, a default value is assigned.

Following are tables for each of the steps used by this workflow where parameters are defined:

Parameters Defined in this Step: Get WebLogic Call-Wrappers

Parameter Name	Default Value	Required	Description
BEA Home	no default	required	Fully qualified path to the middleware home directory that contains the WebLogic 11g and 12c installation. For example: <code>/opt/oracle/weblogic</code>
WLS Install Home	no default	required	Fully qualified path to the directory where WebLogic Server will be installed. For example: <code>/opt/oracle/weblogic/wlserver12.1</code>

Additional Parameters Defined in this Step: Increase WebLogic Domain Span

Parameter Name	Default Value	Required	Description
Local Domain Path	no default	required	Path to the local domain. If the specified path is a relative path, it is assumed to be relative to BEA Home. For example: <code>/opt/oracle/weblogic/user_projects/domains/base_domain</code> where <code>/opt/oracle/weblogic</code> is the BEA Home.
Local Template Path	no default	required	Path to the local template directory or the path to a template file. If the specified path is a relative path, it is assumed to be relative to BEA Home. For example: <code>/opt/oracle/weblogic/user_projects/domains/base_domain.jar</code> where <code>/opt/oracle/weblogic</code> is the BEA Home.
Remote Addresses	no default	required	Comma-delimited list of hosts (DNS addresses or IP addresses) that the domain will span.
Remote Domain Path	no default	optional	Path where the domain will be placed on the remote machine. If the specified path is a relative path, it is assumed to be relative to BEA Home.
Remote Template Path	no default	optional	Path to the remote template directory or the path to a template file. If the specified path is a relative path, it is assumed to be relative to BEA Home. This parameter defaults to Local Template Path.

Additional Parameters Defined in this Step: Start WebLogic Cluster

Parameter Name	Default Value	Required	Description
Admin Server Port	no default	optional	The non-SSL port on which the WebLogic 11g and 12c Administration Server will run.
Cluster Name	no default	required	The name of the new cluster. For example: ClusterAppServer.
WLST Call Wrapper	no default	required	<p>Command that will invoke the WebLogic Scripting Tool (WLST). For example:</p> <pre>su <user> /opt/oracle/WebLogic/install/common/bin/wlst.sh</pre> <p>The fully qualified path will vary depending on where you installed the product. The <user> must have appropriate permissions.</p>
Weblogic Admin Password	no default	required	The password that will be used to authenticate with the WebLogic 11g and 12c Administration Server.
WebLogic Admin User	weblogic	required	The WebLogic 11g and 12c administrator account that will be used to authenticate with the Administration Server.

WebLogic - Create Trust and Identity Keystore

This workflow uses the Java keytool to create a Java keystore, generate a key pair, and export the public key. Then the workflow creates a truststore and imports the public key into the newly created truststore. Finally, the workflow creates a certificate request that can be manually sent to a trusted Certificate Authority (CA) to be signed. After the signed certificate is received from the CA, you can manually import it into the existing truststore.

Tip: This workflow is not exclusive to WebLogic 11g and 12c. The workflow uses a generic Java keytool, allowing it to create the keystore and truststore for application servers, such as IBM WebSphere Application Server Network Deployment.

To use this workflow in your environment, see the following information:

Topic	Information Included
"Prerequisites for this Workflow"	List of prerequisites that must be satisfied before you can run this workflow
"How this Workflow Works"	Information about what the workflow does, including validation checks performed, steps executed, and a high-level process flow
"How to Run this Workflow"	Instructions for running this workflow in your environment
"Sample Scenario"	Examples of typical parameter values for this workflow
Parameters	List of input parameters for this workflow

Prerequisites for this Workflow

Be sure that the following prerequisites are satisfied before you run the ["WebLogic - Create Trust and Identity Keystore"](#) workflow:

- The latest DMA solution packs require the latest DMA platform. To use the latest solution packs, update the DMA platform. DMA 10.40 solution packs are supported on DMA 10.40 (and later).
- You have installed the Application Server Provisioning Solution Pack.
- This workflow is supported on the following Java installations: Java 1.6.x and Java 1.7.x

For more information about prerequisites for WebLogic 11g and 12c, refer to the [WebLogic Product Documentation](#).

How this Workflow Works

The following information describes how the "WebLogic - Create Trust and Identity Keystore" workflow works:

Overview

The workflow does the following:

- Creates the Java keystore.
- Exports the public key out of the keystore and imports it into the truststore. Creates another file with the trusted certificates.
- Creates a certificate request that you can manually send to a Certificate Authority (CA).

Note: Most users wait to receive the signed certificate request back from the CA, but you can use a public certificate in the meantime.

- *Optional:* Imports the root CA certificate and the Intermediate Certificate into the truststore.

Note: If you do not import certificate when you run this workflow, you can also import it manually later.

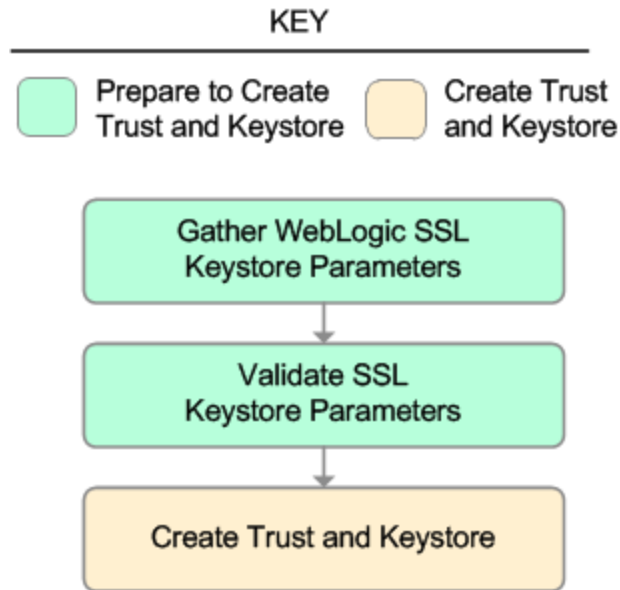
Validation Checks Performed

Much of the validation centers on the input parameters:

- Required parameters have values specified.
- The Java Home version is 1.6 or greater.
- If Intermediate CA Alias is specified, Intermediate CA File Location is a valid existing path with a valid filename. If Intermediate CA File Location is specified, Intermediate CA Alias is specified.
- Certificate Location is a valid path.
- KeyStore Location Directory, Root CA File Location, and TrustStore Location are valid paths with valid filenames.
- KeySize and Validity are integers.

Steps Executed

The WebLogic - Create Trust and Identity Keystore workflow includes the following steps. Each step must complete successfully before the next step can start. If a step fails, the workflow reports a failure and all subsequent steps are skipped.



Steps Used in WebLogic - Create Trust and Identity Keystore

Workflow Step	Description
Gather WebLogic SSL Keystore Parameters	This step gathers all required parameters to create the SSL keystore, truststore, key pairs, exports/imports public key, to import the root CA and intermediate CA, and to create the certificate request.
Validate SSL Keystore Parameters	This step validates and prepares the parameters to create the SSL keystore, truststore, key pairs, exports/imports public key, to import the root CA and intermediate CA, and to create the certificate request.
Create Trust and Keystore	This step creates the SSL keystore, truststore, key pairs, and exports/imports public key. The step imports the root CA and intermediate CA. The step creates the certificate request.

For parameter descriptions and defaults, see ["Parameters for WebLogic - Create Trust and Identity Keystore"](#).

How to Run this Workflow

The following instructions show you how to customize and run the ["WebLogic - Create Trust and Identity Keystore"](#) workflow in your environment.

The workflow provides default values for some parameters. These default values are usually sufficient for a "typical" installation. You can override the defaults by specifying parameter values in the deployment.

Note: Before following this procedure, review the ["Prerequisites for this Workflow"](#) on page 1038, and ensure that all requirements are satisfied.

To use the WebLogic - Create Trust and Identity Keystore workflow:

1. Create a deployable copy of the workflow.
2. Determine the values that you will specify for the following parameters:

Input Parameters for Gather WebLogic SSL Keystore Parameters

Parameter Name	Default Value	Required	Description
Cert Location	no default	required	Fully qualified directory path where the certificate and certificate request will be created. For example: /opt/app/ssl/
Dname Suffix	no default	required	The suffix of the Distinguished Name (DN) that will uniquely identify an entity in an X.509 certificate. The CN will be generated from the server name. For example: OU=Software, O=HP, L=Fort Collins, ST=Colorado, C=US
Intermediate CA Alias	no default	optional	Name or label to uniquely identify the Intermediate CA in the truststore. For example: intermediateca
Intermediate CA File Location	no default	optional	Fully qualified file path where the Intermediate CA is located. For example: /opt/app/ssl/intermediateca.crt
Java Home	no default	required	Fully qualified path to the JAVA_HOME that the keytool uses to create the SSL configuration. For example: /opt/app/jdk1.6.0_35
KeySize	2048	required	Key size or length (in bits) that will be used when creating the Java keystore. For example: 2048
KeyStore	no	required	Fully qualified directory path where the Java keystore will

Input Parameters for Gather WebLogic SSL Keystore Parameters, continued

Parameter Name	Default Value	Required	Description
Location	default		be created. For example: /opt/app/ssl
KeyStore Passphrase	no default	required	Keystore password used to create the keystore and export certificate.
PrivateKey Passphrase	no default	required	Password used to protect the private key in the keystore.
Root CA Alias	no default	required	Name or label to uniquely identify the Root CA in the truststore. For example: rootca
Root CA File Location	no default	required	Fully qualified file path where the Root CA is located. For example: /opt/app/ssl/rootca.crt
TrustStore Location	no default	required	Fully qualified directory path where the Java truststore will be created. For example: /opt/app/ssl
Validity	no default	required	The number of days that the certificate is valid. For example: 365

Note: This is the minimum set of parameters required to run this workflow. You may need to expose additional parameters depending on your objectives.

See ["Parameters for WebLogic - Create Trust and Identity Keystore" on page 1046](#) for detailed descriptions of all input parameters for this workflow, including default values.

- In the workflow editor, expose any additional parameters that you need. You will specify values for those parameters when you create the deployment.
- Save the changes to the workflow (click **Save** in the lower right corner).
- Create a new deployment.
- On the Parameters tab, specify values for the required parameters listed in step 2 and any additional parameters that you have exposed. You do not need to specify values for those parameters whose default values are appropriate for your environment.
- On the Targets tab, specify one or more targets for this deployment.

Note: The target for this deployment should be set to all the servers that are involved in your WebLogic 11g and 12c installation.

8. Save the deployment (click **Save** in the lower right corner).
9. Run the workflow using this deployment.

To verify the results:

The workflow will complete and report SUCCESS on the Console if it has run successfully. If an error occurs during the workflow execution, the error will be logged, and the workflow terminates in the FAILURE state.

Optional: If you want to further verify the results:

Make sure that the keystore, truststore, public key, and certificate request exist.

To do after running this workflow:

Submit the certificate signing request to your CA. The CA will provide instructions for submitting this request.

In response to your request, the CA will send you a digitally signed server certificate via email. Your CA may also send you the root certificate and any intermediate certificates required. Your CA will provide instructions for importing the root and any intermediate certificates into the keystore.

Sample Scenario

It is very straightforward to run the ["WebLogic - Create Trust and Identity Keystore"](#) workflow. This topic shows you typical parameter values to use.

Typical parameters

Input Parameters for Gather WebLogic SSL Keystore Parameters

Parameter Name	Example Value	Description
Cert Location	see description	Fully qualified directory path where the certificate and certificate request will be created. For example: /opt/app/ssl/
Dname Suffix	see description	The suffix of the Distinguished Name (DN) that will uniquely identify an entity in an X.509 certificate. The CN will be generated from the server name. For example: OU=Software, O=HP, L=Fort Collins, ST=Colorado, C=US
Intermediate CA Alias	intermediateca	Name or label to uniquely identify the Intermediate CA in the truststore. For example: intermediateca
Intermediate CA File Location	see description	Fully qualified file path where the Intermediate CA is located. For example: /opt/app/ssl/intermediateca.crt
Java Home	see description	Fully qualified path to the JAVA_HOME that the keytool uses to create the SSL configuration. For example: /opt/app/jdk1.6.0_35
KeySize	2048	Key size or length (in bits) that will be used when creating the Java keystore. For example: 2048
KeyStore Location	/opt/app/ssl	Fully qualified directory path where the Java keystore will be created. For example: /opt/app/ssl
KeyStore Passphrase	kspassword	Keystore password used to create the keystore and export certificate.
PrivateKey Passphrase	pkpassword	Password used to protect the private key in the keystore.
Root CA Alias	rootca	Name or label to uniquely identify the Root CA in the truststore. For example: rootca
Root CA File Location	see description	Fully qualified file path where the Root CA is located. For example: /opt/app/ssl/rootca.crt

Input Parameters for Gather WebLogic SSL Keystore Parameters, continued

Parameter Name	Example Value	Description
TrustStore Location	/opt/app/ssl	Fully qualified directory path where the Java truststore will be created. For example: /opt/app/ssl
Validity	365	The number of days that the certificate is valid. For example: 365

Be sure that the default values for all remaining input parameters are appropriate for your environment (see ["Parameters for WebLogic - Create Trust and Identity Keystore"](#)).

Parameters for WebLogic - Create Trust and Identity Keystore

The following tables describe the required and optional input parameters for this workflow. Some of these parameters may not be initially visible in a deployment. For some parameters, if you do not specify a value for a parameter, a default value is assigned.

Following is a table for the sole step used by this workflow where parameters are defined:

Parameters Defined in this Step: Gather WebLogic SSL Keystore Parameters

Parameter Name	Default Value	Required	Description
Cert Location	no default	required	Fully qualified directory path where the certificate and certificate request will be created. For example: /opt/app/ssl/
Dname Suffix	no default	required	The suffix of the Distinguished Name (DN) that will uniquely identify an entity in an X.509 certificate. The CN will be generated from the server name. For example: OU=Software, O=HP, L=Fort Collins, ST=Colorado, C=US
Intermediate CA Alias	no default	optional	Name or label to uniquely identify the Intermediate CA in the truststore. For example: intermediateca
Intermediate CA File Location	no default	optional	Fully qualified file path where the Intermediate CA is located. For example: /opt/app/ssl/intermediateca.crt
Java Home	no default	required	Fully qualified path to the JAVA_HOME that the keytool uses to create the SSL configuration. For example: /opt/app/jdk1.6.0_35
KeySize	2048	required	Key size or length (in bits) that will be used when creating the Java keystore. For example: 2048
KeyStore Location	no default	required	Fully qualified directory path where the Java keystore will be created. For example: /opt/app/ssl
KeyStore Passphrase	no default	required	Keystore password used to create the keystore and export certificate.
PrivateKey Passphrase	no default	required	Password used to protect the private key in the keystore.
Root CA Alias	no default	required	Name or label to uniquely identify the Root CA in the truststore. For example: rootca
Root CA File Location	no default	required	Fully qualified file path where the Root CA is located.

Parameters Defined in this Step: Gather WebLogic SSL Keystore Parameters, continued

Parameter Name	Default Value	Required	Description
			For example: /opt/app/ssl/rootca.crt
TrustStore Location	no default	required	Fully qualified directory path where the Java truststore will be created. For example: /opt/app/ssl
Validity	no default	required	The number of days that the certificate is valid. For example: 365

WebLogic - Code Release

This workflow automates application deployments in Oracle WebLogic Server. In addition to deployment automation, this workflow can update JVM Generic Arguments and JVM System Properties on the Web Server, and also provides install options for application deployments.

Some install options are provided as parameters for the workflow, or, users can specify install options within a file for each of the applications to be deployed (Note that user-specified parameter values take the highest precedence). This workflow provides application deployment verification by providing the URLs. For successful application deployments, verifications and a list of the applications are maintained in the history file. In cases of unsuccessful application deployments, the workflow rolls back the deployment and restores the last successfully deployed application (if any).

The supported applications are of type :

- .war files
- .ear files

To use this workflow in your environment, see the following information:

Topic	Information Included
"Prerequisites for this Workflow"	List of prerequisites that must be satisfied before you can run this workflow
"How this Workflow Works"	Information about what the workflow does, including validation checks performed, steps executed, and a high-level process flow
"How to run this workflow"	Instructions for running this workflow in your environment
"Sample Scenario"	Examples of typical parameter values for this workflow
Parameters	List of input parameters for this workflow

Prerequisites for this Workflow

Be sure that the following prerequisites are satisfied before you run the WebSphere - Code Release workflow.

Product Platform

This workflow is available to automate application deployments for WebLogic Server 11g and 12C.

Dependencies

- You must have a working WebLogic Application Server on a standalone setup (Provisioning the WebLogic Software and Creating the Domain and Admin Server.)
- You must run the Discover WebLogic workflow before you run this workflow. The Discover WebLogic workflow audits the server's physical environment for WebLogic cells, clusters, and application servers and then stores the configuration information in the DMA environment.

For more information about prerequisites for WebLogic, refer to the WebLogic [Product Documentation](#).

How this Workflow Works

The following information describes how the WebLogic - Code Release workflow works:

Overview

This workflow does the following things in the order shown:

1. Initially, the workflow inputs all parameters, set defaults for optional parameters, and validates all parameters. If input files do not exist in the specified locations, they are downloaded from the software repository. The workflow performs a checksum to verify that the archive files should be deployed in the Application Server on a standalone setup.
2. Next, the workflow creates the installation options and the call wrapper that will be used to execute commands within a WebLogic environment. The workflow updates the setting and then creates a backup. The workflow deploys the specified Application Archive files in the Application Server on a standalone setup.
3. If the application deployment succeeds, the workflow tests the URLs for the web servers and copies the application archives.
4. If the application deployment fails, the workflow rolls back the deployment and restores the last successfully deployed application (if any).
5. Finally, the workflow cleans up downloaded files based on the Cleanup on Success and Cleanup on Failure parameters.

Validation Checks Performed

The workflow performs the following checks on the input parameters:

Enable Security	Must be true or false
If Enable Security is true	WebLogic Admin Username and Password must be specified
WebLogic Admin Username	Cannot contain the following characters / \ * , : ; = + ? < > & % ' " [] # \$ ^ { } and also cannot begin with a dash (-), period (.), or space ()
WebLogic Admin Password	Cannot begin with a dash (-) and cannot contain a space ()
Code Release Staging Location Code Release History Location	Must be valid absolute paths Cannot have the same values
Application Archive File List Md5 Checksum	There must be a checksum for each Application Archive file The Application Archive files must be type .ear or .war and have valid absolute paths Checksums must be valid hexadecimal numbers

The WebLogic - Code Release workflow also checks the environment for the following:

- The WebLogic container type is APPLICATION_SERVER
- The WebLogic Home exists

Steps Used in the WebLogic - Code Release Workflow

Workflow Step	Description
Gather Parameters for WebLogic Code Release	This step gathers mandatory input parameters (user-provided) used to deploy a list of application archives in a Oracle Weblogic Application Server on a standalone setup.
Gather Advanced Parameters for WebLogic Code Release	This step gathers the advanced input parameters (user-provided) used to deploy an application archive for a WebLogic Application Server. Input parameters specified in this step are optional. Appropriate default values are specified.
Validate Parameters for WebLogic Code Release	This step validates the basic and advanced parameters provided by the user, and checks the prerequisites for deploying a list of application archives for an Oracle WebLogic Application Server on a standalone setup.
Check File Download	<p>This step checks for the existence of a file before downloading from the Expert Engine. Specifically, it:</p> <ul style="list-style-type: none"> • Checks to ensure that the file is in the expected location. • If file is not in the expected location, generates a list of files for file download. <p>Note: The Target Directory parameter is set to the directory of the first file in the list not found.</p>
Download Software	This step downloads a list of files to a specified location on the target server.
Validate Checksum for Archive File	This step verifies the checksum for the archive files and archive setting file (if any) to ensure that the file has not changed and that the correct archives are deployed in the Application Server.
Create Install Options File for Application Archives	This step creates a setting file that includes the install options for the list of application archive files being deployed by the application server.
Get WebLogic Call Wrappers	This step creates the necessary call wrapper to call <code>wlst</code> to execute certain operations within a given Weblogic environment.
Update JVM Settings for WebLogic Code Release	This step updates the JVM setting of the Oracle WebLogic Application server. It also performs a backup of the Oracle WebLogic profile configuration.
Deploy Application Archive for WebLogic Code Release	This step deploys the list of application archives in the Oracle WebLogic Application Server on the specified target servers.
If the application deployment succeeds, the following steps are executed	
Verify URLs of Web Server Applications	This step verifies that the URLs are working, and looks for return status code values of 200 for success.
Copy Application	This step copies the list of files from the staging location to the history location.

Steps Used in the WebLogic - Code Release Workflow, continued

Workflow Step	Description
Archives to History	
Cleanup Downloaded Files	For workflow success—and if Cleanup on Success is set to True (default)—this step removes all downloaded files and archives. Dependencies: Run as file/directory owner.
If the application deployment fails, the following steps are executed	
Rollback JVM Settings for WebLogic Code Release	This step restores a backup of the Oracle WebLogic profile configuration.
Undeploy Application Archives for WebLogic Code Release	This step uninstalls the list of application archives from an Oracle WebLogic Application Server on a standalone setup.
Deploy Application Archives for WebLogic Code Release	This step deploys the list of application archives in the Oracle WebLogic Application Server on the specified target servers.
Cleanup Downloaded Files	For workflow failure—and if Cleanup on Failure is set to True (default)—this step removes all downloaded files and archives. Dependencies: Run as file/directory owner.

How to run this workflow

The following instructions show you how to customize and run the WebLogic - Code Release workflow in your environment.

The workflow provides default values for some parameters. These default values are usually sufficient for a "typical" installation. You can override the defaults by specifying parameter values in the deployment. For details about specific parameter values, see ["Parameters for WebLogic - Code Release" on page 1058](#).

Note: Before following this procedure, review the ["Prerequisites for this Workflow" on page 1048](#), and ensure that all requirements are satisfied.

Before you run this workflow, you can perform the following optional advance configuration to deploy applications WebLogic application servers.

Create a configuration file on the target machine or the SA Server. The file should contain the advanced parameters for all the application servers being deployed. If no configuration file is provided, the target will be defaulted to admin server of the domain. The options that are to be used in this file are listed in the table below.

For example, if you want to deploy example1.war, example2.war, and example3.war onto the managed servers named MS-1, MS-2, and MS-3. The format of the configuration file as an input to the flow must be as the following:

```
example1.war = {
  -appName MyfirstwarFile
  -targets MS-1
  -upload false
}
example2.war = {
  -appName example2
  -targets MS-2,MS-1
  -createPlan false
}
example3.war = {
  Application Name=example3
  Targets=Cluster-1,MS-1,AdminServer
  -altDD None
  -altWlsDD None
  -archiveVersion None
  -upload false
}
```

The options in this file should be in the following format:

Format 1	Format 2	Description
Application Name	-appName	Name of the application or standalone Java Enterprise Edition (Java EE) module that is to be deployed.
Targets	-targets	(Optional) Comma-separated list of the targets. Each target may be qualified with a Java EE module name.
Stage Mode	-stageMode	(Optional) Staging mode for the applications you are deploying. Valid values are stage, nostage, and external_stage.
Plan Path	-planPath	Optional. Name of the deployment plan file. The filename can be absolute or relative to the application directory. This argument defaults to the plan/plan.xml file in the application directory, if one exists.
Alternative Deployment	-altDD	Location of the alternate application deployment descriptor on the

Format 1	Format 2	Description
Descriptor		Administration Server.
Alternative WebLogic Deployment Descriptor	-altWlsDD	Location of the alternate WebLogic application deployment descriptor on the Administration Server.
Archive Version	-archiveVersion	Archive version number
Block	-block	Boolean value specifying whether WLST should block user interaction until the command completes. This option defaults to true.
Cluster Deployment Timeout	-clusterDeploymentTimeout	Time, in milliseconds, granted for a cluster deployment task on this application.
Create Plan	-createPlan	Boolean value indicating that user would like to create a default plan. This option defaults to false.
Default Submodule Targets	-defaultSubmoduleTargets	Boolean value indicating that targeting for qualifying JMS submodules should be derived by the system
Force Undeploy Timeout	-forceUndeployTimeout	Force undeployment timeout value.
Graceful Ignore Sessions	-gracefulIgnoreSessions	Boolean value specifying whether the graceful production to admin mode operation should ignore pending HTTP sessions. This option defaults to false and only applies if gracefulProductionToAdmin is set to true.
Graceful Production To Admin	-gracefulProductionToAdmin	Boolean value specifying whether the production to Admin mode operation should be graceful. This option defaults to false.
Implementation Version	-libImplVersion	Implementation version of the library, if it is not present in the manifest.
Library Module	-libraryModule	Boolean value specifying whether the module is a library module. This option defaults to false.
Specification Version	-libSpecVersion	Specification version of the library, if it is not present in the manifest
Plan Version Number	-planVersion	Plan version number
Retire Gracefully	-retireGracefully	Retirement policy to gracefully retire an application only after it has completed all in-flight work. This policy is only meaningful for stop and redeploy operations and is mutually exclusive to

Format 1	Format 2	Description
		the retire timeout policy.
Retire Timeout	-retireTimeout	Time (in seconds) WLST waits before retiring an application that has been replaced with a newer version. This option default to -1, which specifies graceful timeout.
Security Model	-securityModel	Security model. Valid values include:DDOnly, CustomRoles, CustomRolesAndPolicies, andAdvanced.
Security Validation Enabled	-securityValidationEnabled	Boolean value specifying whether security validation is enabled.
Sub Module Targets	-subModuleTargets	Submodule level targets for JMS modules. For example,submod@mod-jms.xml@target submoduleName@target.
Timeout	-timeout	Time (in milliseconds) that WLST waits for the deployment process to complete before canceling the operation. A value of 0 indicates that the operation will not time out. This argument defaults to 300,000 ms (or 5 minutes).
Version Identifier	-versionIdentifier	Version identifier
Upload	-upload	Boolean value specifying whether the application files are uploaded to the WebLogic Server Administration Server's upload directory prior to deployment. Use this option when the Administration Server cannot access the application files through the file system. This option defaults to false.

You can select any advanced option from either list1 or list2.

If you select an option from list 1, the value has to be separated by an '=' sign, for example: Application Name=example3.

If you select an option from list 2, the value has to be separated by a space character, for example: - appName example.

Sample Scenario

This topic shows you typical parameter values for different use cases for the WebLogic – Code Release workflow. For a complete list of all parameters used in this workflow, including default values,

see ["Parameters for WebLogic - Code Release" on page 1058](#).

Scenario: Install an application archive (for example stockanalysis.war) on a running Oracle WebLogic Application Server on a standalone setup

In this scenario we will deploy the stockanalysis.war file on a running Oracle WebLogic Application Server. We will install the application using the default installation options. If the application archive files are not present in the Code Release Staging Location, then they will be downloaded from the SA Repository.

In addition to the default options, this flow also provides advanced parameters to specify:

- JVM System properties
- JVM Memory arguments
- Archive Setting File
- Domain path

Parameters Defined in this Step: Gather Parameters for WebLogic- Code Release

Parameter Name	Example Value	Description
Admin Password	Weblogic123	The WebLogic Administrator password.
Admin Server Hostname	myserver.com	The WebLogic Admin Server Hostname or IP address.
Admin Server Port	7001	The port number of the Admin WebLogic Server.
Admin Username	Weblogic	The Admin Username for logging into the WebLogic Server.
Application Archive File List	stockanalysis.war	Comma-separated list of the Application Archive files to be deployed. Example: xxx.war or yyy.ear
BEA Home	/opt/oracle/WebLogic	Fully qualified path of the product installation directory in which WebLogic Server is installed
Code Release History Location	/opt/oracle/weblogic/history	Fully qualified path name of the location where the application archive will be saved (for history purposes) on the target machine. This location cannot be the same as the Code Release Staging Location.
Code Release Staging	/tmp/	Fully qualified path name of the location where the application archive will be saved on the target

Parameters Defined in this Step: Gather Parameters for WebLogic- Code Release , continued

Parameter Name	Example Value	Description
Location		machine. This location cannot be the same as the Code Release History Location.
Md5 Checksum	477e994e9d457ad2214a3d36b1bb16b	Comma-separated list of the MD5 Checksum of the Application Archive files to be deployed. Please provide the Checksum for the Archive File if listed.
Test URLs	http://<server:port>/stockanalysis/<xyx.html>	Comma-separated list of URLs used to test whether or not the list of applications deployed successfully. Example: http://mytestdb.com, http://yourtest.com
WLS Install Home	/opt/oracle/WebLogic/wlserver_10.30	Fully qualified path to the Middleware Home directory that will contain this installation. For instance /opt/oracle/WebLogic/wlserver_10.30

Parameters Defined in this Step: Gather Advanced Parameters for WebLogic - Code Release

Parameter Name	Value	Description
Archive Setting File	archive.setting	The file containing the install options for all the archive file.
Domain Path	/opt/oracle/weblogic/domains/mydomain	Fully qualified path of the domain under which the Admin server resides. Example: /opt/oracle/weblogic/user_projects/domains/mydomain_name/
JVM Memory Arguments	-Xms256m -Xmx512m	Specifies the JVM memory arguments. Provide values as standard JVM settings with a space as delimiter. Example: -Xms256m -Xmx512m
JVM System Properties	stockanalysis_home, /opt/stockanalysis/bin, Home path for the stock analysis	Specifies the JVM System Properties. Provide string in the following format: DPropertyName=PropertyValue

Parameters for WebLogic - Code Release

The following tables describe the required and optional input parameters for this workflow. For most parameters, if you do not specify a value for a parameter, a default value is assigned.

Parameters Defined in this Step: Gather Parameters for WebLogic - Code Release

Parameter Name	Default Value	Required	Description
Admin Password	no default	required	The Administrator password for logging into the WebLogic Server.
Admin Server Hostname	no default	required	The Admin Server Hostname.
Admin Server Port	7001	required	The port number of the Admin WebLogic Server
Admin Username	no default	required	The Admin Username for logging into the WebLogic Server.
Application Archive File List	no default	required	Comma separated list of Application Archives to be deployed.
BEA Home	no default	required	Fully qualified path to the product installation directory in which to install WebLogic Server. For instance /opt/oracle/WebLogic.
Code Release History Location	no default	required	Fully qualified path name of the location where the application archive will be saved (for history purposes) on the target machine. This location cannot be the same as the Code Release Staging Location.
Code Release Staging Location	no default	required	Fully qualified path name of the location where the application archive will be saved on the target machine. This location cannot be the same as the Code Release History Location.
Md5 Checksum	no default	required	Comma-separated list of the MD5 Checksum of the Application Archive files to be deployed. Please provide the Checksum for the Archive File if listed.
Test URLs	no default	required	Comma-separated list of URLs used to test whether or not the list of applications deployed successfully. Example: http://mytestdb.com, http://yourtest.com
WLS Install Home	no default	required	Fully qualified path to the Middleware Home directory that will contain this installation. For instance /opt/oracle/WebLogic/wlserver_10.30

Parameters Defined in this Step: Gather Advanced Parameters for WebLogic - Code Release

Parameter Name	Default Value	Required	Description
Archive Setting File	no default	optional	The file containing the install options for all the archive file.

Parameters Defined in this Step: Gather Advanced Parameters for WebLogic - Code Release , continued

Parameter Name	Default Value	Required	Description
Cleanup on Failure	True	optional	Determines whether or not to remove downloaded and extracted files. This parameter also cleans up the installed directory upon failure of the workflow.
Cleanup on Success	True	optional	Determines whether or not to remove downloaded and extracted files. This parameter also cleans up the installed directory upon successful execution of the workflow.
Domain Path	no default	optional	Fully qualified path of the domain under which the Admin server resides. Example: /opt/oracle/weblogic/user_projects/domains/mydomain_name/
JVM Memory Arguments	no default	optional	Specifies the JVM memory arguments. Provide values as standard JVM settings with a space as delimiter. Example: -Xms256m -Xmx512m
JVM System Properties	no default	optional	Specifies the JVM System Properties. Provide string in the following format: DPropertyName=PropertyValue

WebLogic - Create and Configure Datasource

The purpose of this workflow is to create a generic datasource in a Weblogic Application Server . A datasource can be created using drivers installed with the WebLogic server or with the drivers installed in the WebLogic domain by the user.

Note: The third party drivers should be installed on all servers (clusters) on which the datasource will be deployed.

To install third party JDBC Drivers, refer to Oracle WebLogic Server documentation.

Datasources—backend connections to an existing database—allow pooling of connections to the database for fast access, reuse by application components, and abstraction of the database connection information by WebLogic.

Supported vendors

The supported WebLogic application versions are:

- WebLogic application server 11g and 12c.

See [WebLogic Product Documentation](#) to find additional information about WebLogic Server Datasources.

To use this workflow in your environment, see the following information:

Topic	Information Included
"Prerequisites for this Workflow"	List of prerequisites that must be satisfied before you can run this workflow
"How this Workflow Works"	Information about what the workflow does, including validation checks performed, steps executed, and a high-level process flow
"How to Run this Workflow"	Instructions for running this workflow in your environment
"Sample Scenario"	Examples of typical parameter values for this workflow
Parameters	List of input parameters for this workflow

Prerequisites for this Workflow

Be sure that the following prerequisites are satisfied before you run the WebLogic - Create and Configure Datasource workflow.

Product Platform

This workflow is available for WebLogic 11g and 12c

Dependencies

This workflow has the following dependencies:

- You must have a working WebLogic server version 11g or 12c.
- You must have a domain and an admin server provisioned to run this workflow.
- The database pertaining to the datasource connection must be running, else the deployment of the datasource will fail. The user then has to manually deploy the datasource on the target.
- The datasource uses non-SSL port and WLST to create and deploy a datasource.

For more information about prerequisites for WebLogic, refer to the [WebLogic Product Documentation](#).

How this Workflow Works

The following information describes how WebLogic - Create and Configure Datasource workflow works:

Overview

This workflow does the following things in the order shown:

1. Before creating the WebLogic data source, the workflow prepares and validates all parameters and creates the call wrapper that will be used to execute commands within a WebLogic Application server.
2. Next the workflow uses WLST (WebLogic Scripting Tool) as the core call wrapper and creates the configuration xml for the datasource and deploys it on the servers or clusters in that domain.
3. Finally, the workflow verifies that the connection to the data source was successful.

Validation Checks Performed

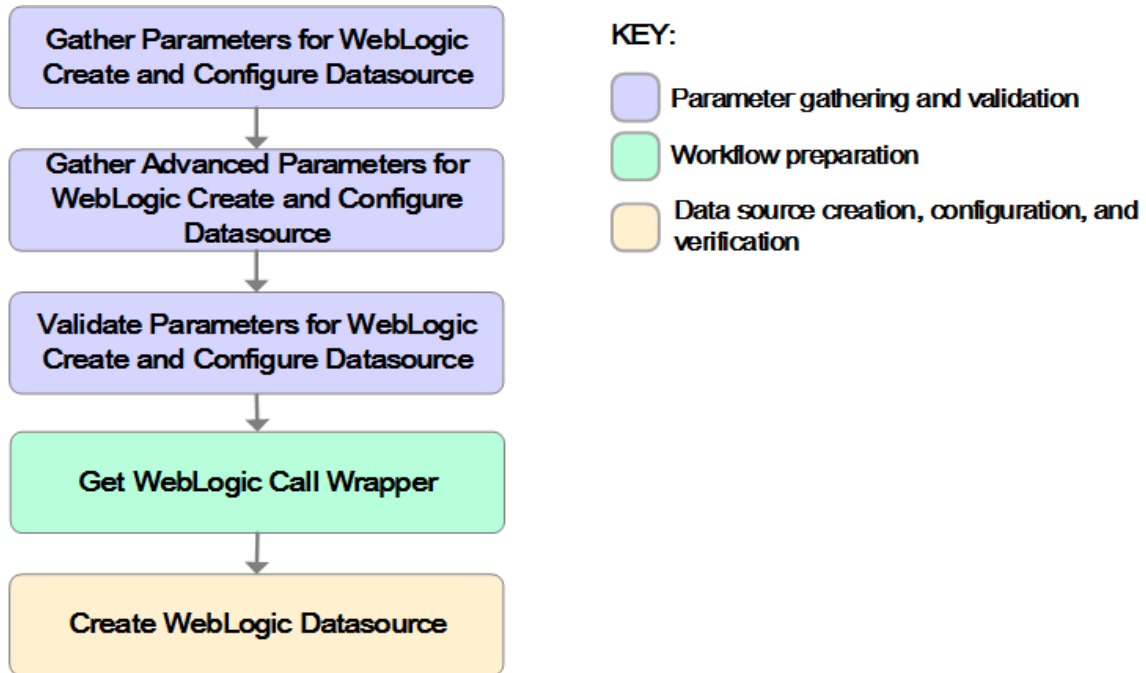
The workflow then performs the following checks on the input parameters:

BEA Home	The WebLogic software installation must exist.
Admin Password Admin Server Host Name Admin Server Port Admin User	Must be specified.
Database Name Database Port Database Server Name	Should be specified when the data source JDBC Connection String be constructed by the workflow.
Database User Database Password	Required to validate the jdbc connection when deploying the data source.
Datasource JNDI	Must be specified. Can be one or more. Comma separated list of JNDI Names.
Datasource Type	Can only be one of the following: Oracle Sybase SQL Server DB2 Informix Other
DS Max Capacity	Must be specified and can be only numeric.
JDBC Connection String JDBC Driver Class JDBC Connection Properties	Required when the Datasource Type is "Other" JDBC Driver Class must be installed on every server to which the data source is deployed. JDBC Connection Properties can be of the form a=b,c=d,e=f,... etc.
XA Datasource Clean Up On Failure	Can only be True or False.
Cluster List Server List	Optional Can take one or more values Comma separated list of values

WLS Install Home	The WebLogic server home must exist.
------------------	--------------------------------------

Steps Executed

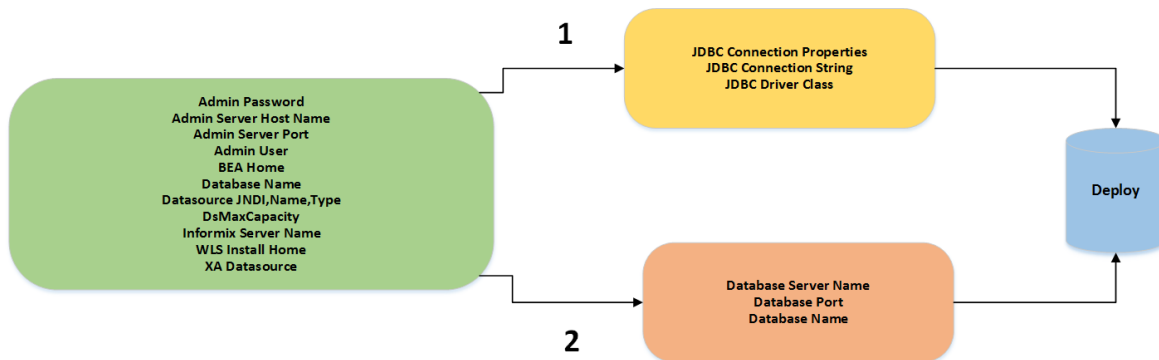
The WebLogic - Create and Configure Datasource workflow includes the following steps. Each step must complete successfully before the next step can start. If a step fails, the workflow reports a failure and all subsequent steps are skipped.



Steps Used in the WebLogic - Create and Configure Datasource Workflow

Workflow Step	Description
Gather Parameters for Weblogic Create and Configure Datasource	This step performs the following actions to facilitate the execution of subsequent steps in the workflow: Prepares the parameters needed to create a datasource in Weblogic Application Server . Return Code: 0 = Step ran successfully 1 = Step failed.
Gather Advanced Parameters for Weblogic Create and Configure Datasource	This step prepares the parameters needed to create a Datasource in Weblogic Application Server . Return Code: 0 = Step ran successfully 1 = Step failed.
Validate Parameters for Weblogic Create and Configure Datasource	This step prepares the parameters needed to create a Datasource in Weblogic Application Server . Return Code: 0 = Step ran successfully 1 = Step failed.
Get WebLogic Call Wrappers	This step creates the necessary call wrapper to call list to execute certain operations within a given Weblogic environment. Return Code: 0 = Step ran successfully 1 = Step failed.
Create Weblogic DataSource	Creates a generic datasource in a weblogic application server. Return Code: 0 = Step ran successfully 1 = Step failed.

For parameter descriptions and defaults, see ["Parameters for WebLogic - Create and Configure Datasource" on page 1078](#)



Path 2: This is used to create a datasource with the JDBC drivers which are part of the standard WebLogic installation. The JDBC connection string is constructed from the user given values to the three parameters as shown.
 Path 1: This is used to create a datasource with the third party JDBC drivers which are installed by the user in their WebLogic environment.

How to Run this Workflow

The following instructions show you how to customize and run the WebLogic - Create and Configure Datasource workflow in your environment.

The workflow provides default values for some parameters. These default values are usually sufficient for a "typical" installation. You can override the defaults by specifying parameter values in the deployment. You can also expose additional parameters in the workflow, if necessary, to accomplish more advanced scenarios. Any parameters not explicitly specified in the deployment will have the default values listed in ["Parameters for WebLogic - Create and Configure Datasource" on page 1078](#)

Note: Before following this procedure, review the ["Prerequisites for this Workflow" on page 1061](#), and ensure that all requirements are satisfied.

To use the WebLogic - Create and Configure Datasource workflow:

1. Create a deployable copy of the workflow.
2. Determine the values that you will specify for the following parameters: show

Gather Parameters for WebLogic - Create and Configure Datasource Parameters

Parameter Name	Default Value	Required	Description
Admin Password	No default	Required	This password will be used to authenticate the Weblogic Admin Server.
Admin Server Host Name	No default	Required	This is the hostname or IP address that the Weblogic Admin Server will run on.
Admin Server Port	No default	Required	This will be the non SSL port that the WebLogic Admin Server will run on.
Admin User	None	Yes	This is the WebLogic administrator username used to connect to the Admin Server.
BEA Home	None	Yes	Fully qualified path to the product installation directory in which WebLogic Server is placed for Ex. /opt/oracle/weblogic
Database Name	None	Yes	This will be the database instance name that will be used in the connection string. Example: For MS SQL it will be "ServerName\InstanceName".
Database Password	None	Yes	This is the database password that the connection will use to authenticate the database.
Database Port	None	Yes	This is the port that the database is listening on.
Database Server Name	None	Yes	This is the hostname or IP address that the database is installed on.

Gather Parameters for WebLogic - Create and Configure Datasource Parameters , continued

Parameter Name	Default Value	Required	Description
Database User	None	Yes	This is the database user that the connection will use to authenticate the database.
Datasource JNDI	None	Yes	This will be the comma separated list of JNDI Names, which will be used for datasource creation.
Datasource Name	None	Yes	Unique name that will identify the datasource in the WebLogic domain.
Datasource Type	None	Yes	Type of the database on which the datasource will be deployed. The options are "Sybase," "Oracle," "SQLserver," "DB2," "Informix," "Other".
DsMaxCapacity	None	Yes	The maximum number of connection pool threads for the datasource.
Informix Server Name	None	No	Required when the workflow is used to create an Informix datasource.
JDBC Connection Properties	None	No	If the Datasource Type is "other", then this value will be used to initialize the JDBC Connection properties of the Datasource, It can take values of the form a=b,c=d,e=f etc
JDBC Connection String	None	No	If the Datasource Type is "other", then this value will be used to initialize the JDBC Connection String of the datasource.
JDBC Driver Class	None	No	If the Datasource Type is "other," then this value will be used to initialize the JDBC Driver Class of the Datasource.
WLS Install Home	None	Yes	Fully qualified path to the Middleware Home directory that will contain this installation. For instance /opt/oracle/WebLogic/wlserver_12.1.
XA Datasource	False	Yes	"True" refers that the current datasource is of type XA which supports two phase commit. "False" refers to Non- Xa with single phase commit.

Gather Advanced Parameters for WebLogic Create and Configure Datasource

Parameter Name	Default Value	Required	Description
Clean Up On Failure	True	Yes	Specifies if the datasource is to be removed upon failure.
Cluster List	None	No	Comma separated list of cluster names on which datasource will be deployed. If Server_list is empty as well, then the datasource will be created and deployed on all managed servers.

Gather Advanced Parameters for WebLogic Create and Configure Datasource, continued

Parameter Name	Default Value	Required	Description
Current Target Only	False	No	If True , datasource will be created and deployed only on the current target on which this code is running. Else, it will be False.
Server List	No default	Optional	Comma seperated list of servers names on which the datasource will be be deployed. If Cluster_list is empty as well, then the datasource will be created and deployed on all managed servers.

Tip: To avoid having to re-enter passwords whenever they change, you can create a policy to provide them to the workflow.

Note: This is the minimum set of parameters required to run this workflow. You may need to expose additional parameters depending on your configuration management objectives.

See ["Parameters for WebLogic - Create and Configure Datasource" on page 1078](#) for detailed descriptions of all input parameters for this workflow, including default values.

3. In the workflow editor, expose any additional parameters that you need. You will specify values for those parameters when you create the deployment.
4. Save the changes to the workflow.
5. Create a new deployment.
6. On the Parameters tab, specify values for the required parameters listed in step 2 and any additional parameters that you have exposed. You do not need to specify values for those parameters whose default values are appropriate for your environment.
7. On the Targets tab, specify one or more targets for this deployment.
8. Save the deployment (click **Save** in the lower right corner).
9. Run the workflow using this deployment.

To verify the results:

The workflow will complete and report SUCCESS on the Console if it has run successfully. If an error occurs during workflow execution, the error is logged, and the workflow terminates in the FAILURE state.

Optional: If you want to further verify the results:

Use the WebLogic user interface to check that the data source is connected.

Sample Scenario

This topic shows you typical parameter values for different use cases for the WebLogic - Create and Configure Datasource workflow. For a complete list of all parameters used in this workflow, including default values, see ["Parameters for WebLogic - Create and Configure Datasource" on page 1078](#).

The sample scenarios assume that Web Service URL has the value of DMA.URL. This is the default value mapped from the DMA metadata.

Tip: To avoid having to re-enter passwords whenever they change, you can create a policy to provide them to the workflow.

Scenario 1: To create an Oracle data source using connection pool data source

This use case will create an Oracle data source using connection pool data source. This example does not enable security.

Gather Parameters for WebLogic - Create and Configure Datasource

Parameter Name	Example Value	Description
Admin Password	weblogic123	This password will be used to authenticate the WebLogic Admin Server.
Admin Server Host Name	myweblogic.mycompany.mydomain.com (Can be hostname or IP)	This is the hostname or IP address that the WebLogic Admin Server will run on.
Admin Server Port	7001	This will be the non-SSL port that the WebLogic Admin Server will run on.
Admin User	WebLogic	This is the WebLogic administrator username used to connect to the Admin Server.
BEA Home	/opt/oracle/weblogic	Fully qualified path to the product installation directory in which the WebLogic server is placed. For instance /opt/oracle/webLogic
Database Name	test	This will be the database instance name that will be used in the connection string.
Database Password	dbpass123	This is the database password that the connection will use to authenticate with the database.
Database Port	1521	This is the port that the database is listening on.
Database Server Name	mydatabase.mycompany.mydomain.com (Can be hostname or IP)	This the hostname or IP address that the database is installed on.

Gather Parameters for WebLogic - Create and Configure Datasource, continued

Parameter Name	Example Value	Description
Database User	dma	This is the database user that the connection will use to authenticate the database.
Datasource JNDI	orcl_jndi_name1 (can be "orcl_jndi_1,orcl_jndi_2,...")	This will be comma seperated list of values that will be used as JNDI names bound with the datasource.
Datasource Name	ds_oracl	A unique name that identifies this datasource in the WebLogic domain.
Datasource Type	Oracle	This parameter sets the type of datasource that will be created. Options are "Sybase", "Oracle", "SQLserver", "DB2", "Informix", "Other"
DsMaxCapacity	12	The maximum number of connection pool threads for the datasource.
Informix Server Name	No value	Required when the workflow is used to create a informix datasource.
JDBC Connection Properties	No value	If the Datasource Type is "other," then this value will be used to initialize the JDBC Connection properties of the Datasource. It can take values of the form a=b, c=d, e=f etc
JDBC Connection String	No value	If the Datasource Type is "other," then this value will be used to initialize the JDBC Connection String of the Datasource.
JDBC Driver Class	No value	If the Datasource Type is "other," then this value will be used to initialize the JDBC Driver Class of the Datasource.
WLS Install Home	/opt/oracle/weblogic/wlserver12.1/	Fully qualified path to the Middleware Home directory that will contain this installation. For instance /opt/oracle/WebLogic/wlserver_10.3.
XA Datasource	True	"True" refers that the current datasource is of type XA which supports Two phase commit. "False" refers to Non- Xa with single phase commit.

Gather Advance Parameters for WebLogic Create and Configure Datasource

Parameter Name	Example Value	Description
Clean Up On Failure	True	Specifies if the datasource should be removed upon failure.

Gather Advance Parameters for WebLogic Create and Configure Datasource, continued

Parameter Name	Example Value	Description
Cluster List	Cluster-1,Cluster-2	Comma separated list of cluster names on which datasource will be deployed. If Server_list is empty as well then the datasource will be created and deployed on all managed servers.
Current Target Only	False	If True, the datasource will be created and deployed only on current target on which this code is running and False otherwise.
Server List	Server-2,Server100	Comma separated list of servers names on which datasource will be deployed. If Cluster_list is empty as well, then the datasource will be created and deployed on all the managed servers.

Scenario 2: To create an SQL Server data source using connection pool data source

This use case will create an SQL Server data source using connection pool data source and does not enable security.

Input Parameters for WebLogic - Create and Configure Datasource Parameters

Parameter Name	Example Value	Description
Admin Password	weblogic123	This will be the password that will be used to authenticate the Weblogic Admin Server.
Admin Server Host Name	myweblogic.mycompany.mydomain.com (Can be hostname or IP)	This is the hostname or IP address that the WebLogic Admin Server will run on.
Admin Server Port	7001	This will be the non-SSL port that the WebLogic Admin Server will run on.
Admin User	WebLogic	This is the WebLogic administrator username used to connect to the Admin Server.
BEA Home	/opt/oracle/weblogic	Fully qualified path to the product installation directory in which WebLogic Server is placed. For instance /opt/oracle/WebLogic
Database Name	test	This will be the database instance name that will be used in the connection string.
Database Password	dbpass123	This is the database password that the connection will use to authenticate the database.
Database Port	1402	This is the port that the database is listening on.
Database Server Name	mydatabase.mycompany.mydomain.com (Can be hostname or IP)	This the hostname or IP address that the database is installed on.
Database User	dma	This is the database user that the connection will use to authenticate the database.
Datasource JNDI	sql_jndi_name1 (Can be like "sql_jndi_1,sql_jndi_2,...")	These will be comma separated list of values that will be used as JNDI Names bound with the datasource.
Datasource Name	ds_sql	A unique name that identifies this data source in the WebLogic domain.
Datasource Type	sql server	This parameter sets the type of datasource that will be created. Options are "Sybase", "Oracle", "SQLServer", "DB2", "Informix", "Other"

Input Parameters for WebLogic - Create and Configure Datasource Parameters , continued

Parameter Name	Example Value	Description
DsMaxCapacity	12	The maximum number of connection pool threads for the datasource.
Informix Server Name	No value	Required when the workflow is used to create an informix datasource.
JDBC Connection Properties	No value	If the Datasource Type is "other," then this value will be used to initialize the JDBC Connection properties of the datasource. It can take values of the form a=b, c=d, e=f, etc.
JDBC Connection String	No value	If the Datasource Type is "other," then this value will be used to initialize the JDBC Connection String of the Datasource.
JDBC Driver Class	No value	If the Datasource Type is "other", then this value will be used to initialize the JDBC Driver Class of the Datasource.
WLS Install Home	/opt/oracle/weblogic/wlserver12.1/	Fully qualified path to the Middleware Home directory that will contain this installation. For instance /opt/oracle/WebLogic/wlserver_10.3.
XA Datasource	True	"True" refers that the current datasource is of type XA which supports two phase commit. "False" refers to Non-Xa with single phase commit.

Gather Advance Parameters for WebLogic Create and Configure Datasource

Parameter Name	Example Value	Description
Clean Up On Failure	True	Specifies if the datasource be removed upon failure.
Cluster List	Clusterds1	Comma separated list of cluster names on which the datasource will be deployed. If Server_list is empty as well, then the datasource will be created and deployed on all managed servers.
Current Target Only	False	If True , datasource will be created and deployed only on current target on which this code is running and False otherwise
Server List	Server-2, Server 100	Comma separated list of servers names on which datasource will be deployed. if Cluster_list is empty as well then the datasource will be created and deployed on all managed servers.

Scenario 3: To create a datasource for "Other" database**Input Parameters for WebLogic - Create and Configure Datasource Parameters**

Parameter Name	Example Value	Description
Admin Password	weblogic123	This will be the password that will be used to authenticate the Weblogic Admin Server.
Admin Server Host Name	myweblogic.mycompany.mydomain.com (Can be hostname or IP)	This is the hostname or IP address that the Weblogic Admin Server will run on.
Admin Server Port	7001	This will be the non ssl port that the Weblogic Admin Server will run on.
Admin User	WebLogic	This is the WebLogic administrator username used to connect to the Admin Server
BEA Home	/opt/oracle/weblogic	Fully qualified path to the product installation directory in which WebLogic Server is placed. For instance /opt/oracle/WebLogic.
Database Name	No value	This will be the database instance name that will be used in the connection string
Database Password	dbpass123	This is the database password that the connection will use to authenticate the database.
Database Port	No value	This is the port that the database is listening on.
Database Server Name	No value	This the host name or IP address that the database is installed on.
Database User	DMA	This is the database user that the connection will use to authenticate with the database.
Datasource JNDI	orcl_jndi_name1 (can be "orcl_jndi_1,orcl_jndi_2,....")	This will be comma separated list of values that will be used as JNDI Names bound with the datasource.
Datasource Name	ds_oracl	A unique name that identifies this data source in the WebLogic domain.
Datasource Type	Oracle	This parameter sets the type

Input Parameters for WebLogic - Create and Configure Datasource Parameters, continued

Parameter Name	Example Value	Description
		of datasource that will be created. Options are "Sybase", "Oracle," "SQL Server", "DB2", "Informix", "Other"
DsMaxCapacity	12	The maximum number of connection pool threads for the datasource.
Informix Server Name	No value	Required when the workflow is used to create an Informix datasource.
JDBC Connection Properties	user=dma,portNumber=50000,databaseName=test	If the Datasource Type is "other" , then this value will be used to initialize the JDBC Connection properties of the Datasource. It can take values of the form a=b,c=d,e=f, etc.
JDBC Connection String	jdbc:weblogic:db2://mydbserver.mycompany.com:50000 <<have this in one line>>	If the Datasource Type is "other," then this value will be used to initialize the JDBC Connection String of the Datasource.
JDBC Driver Class	weblogic.jdbcx.db2.DB2DataSource	If the Datasource Type is "other," then this value will be used to initialize the JDBC Driver Class of the Datasource.
WLS Install Home	/opt/oracle/weblogic/wlserver12.1/	Fully qualified path to the Middleware Home directory that will contain this installation. For instance /opt/oracle/WebLogic/wlserver_10.3
XA Datasource	True	"True" refers that the current datasource is of type XA which supports two phase commit. "False" refers to non-Xa with single phase commit.

Gather Advance Parameters for WebLogic Create and Configure Datasource

Parameter Name	Example Value	Description
Clean Up On Failure	True	Specifies if the datasource can be removed upon failure.
Cluster List	Cluster-1,Cluster-	Comma separated list of cluster names on which datasource will be deployed. If Server_list is empty as well, then the datasource will be

Gather Advance Parameters for WebLogic Create and Configure Datasource, continued

Parameter Name	Example Value	Description
	2	created and deployed on all managed servers.
Current Target Only	False	If True, datasource will be created and deployed only on current target on which this code is running and False otherwise.
Server List	Server-2, Server100	Comma separated list of servers names on which datasource will be be deployed. if Cluster_list is empty as well, then the datasource will be created and deployed on all managed servers.

Parameters for WebLogic - Create and Configure Datasource

The following tables describe the required and optional input parameters for this workflow. Most of these parameters are not initially visible in a deployment. For most parameters, if you do not specify a value for a parameter, a default value is assigned.

Parameters Defined in this Step: Validate WebLogic - Create and Configure Datasource

Parameter Name	Default Value	Required	Description
Admin Password	None	Yes	This is the password for the WebLogic Application Server.
Admin Server Host Name	None	Yes	This is the hostname or IP of the Weblogic Admin Server.
Admin Server Port	None	Yes	This is the non SSL port that the WebLogic server will run on.
Admin User	None	Yes	This is the WebLogic administrator username used to connect to the Admin Server.
BEA Home	None	Yes	Fully qualified path to the product installation directory in which WebLogic Server is placed for Ex. /opt/oracle/weblogic
Database Name	None	Yes	This will be the database instance name that will be used in the connection string. Example: For MS SQL it will be "ServerName\InstanceName".
Database Password	None	Yes	This is the database password that the connection will use to authenticate the database.
Database Port	None	Yes	This is the port that the database is listening on.
Database Server Name	None	Yes	This is the hostname or IP address that the database is installed on.
Database User	None	Yes	This is the database user that the connection will use to authenticate the database.
Datasource JNDI	None	Yes	This will be the comma separated list of JNDI Names, which will be used for datasource creation.
Datasource Name	None	Yes	Unique name that will identify the datasource in the WebLogic domain.
Datasource Type	None	Yes	Type of the database on which the datasource will be deployed. The options are "Sybase," "Oracle," "SQLserver," "DB2," "Informix," "Other".
DsMaxCapacity	None	Yes	The maximum number of connection pool threads for the datasource.
Informix Server Name	None	No	Required when the workflow is used to create an Informix datasource.
JDBC Connection	None	No	If the Datasource Type is "other", then this value will be used to initialize the JDBC Connection properties of the

Parameters Defined in this Step: Validate WebLogic - Create and Configure Datasource , continued

Parameter Name	Default Value	Required	Description
Properties			Datasource, It can take values of the form a=b,c=d,e=f etc
JDBC Connection String	None	No	If the Datasource Type is "other", then this value will be used to initialize the JDBC Connection String of the datasource.
JDBC Driver Class	None	No	If the Datasource Type is "other," then this value will be used to initialize the JDBC Driver Class of the Datasource.
WLS Install Home	None	Yes	Fully qualified path to the Middleware Home directory that will contain this installation. For instance /opt/oracle/WebLogic/wlserver_12.1.
XA Datasource	False	Yes	"True" refers that the current datasource is of type XA which supports two phase commit. "False" refers to Non-Xa with single phase commit.
Clean Up On Failure	True	Yes	Specifies if the datasource is to be removed upon failure.
Cluster List	None	No	Comma separated list of cluster names on which datasource will be deployed. If Server_list is empty as well, then the datasource will be created and deployed on all managed servers.
Current Target Only	False	No	If True, datasource will be created and deployed only on the current target on which this code is running. Else, it will be False.
Server List	None	No	Comma separated list of servers names on which the datasource will be deployed. If Cluster_list is empty as well, then the datasource will be created and deployed on all managed servers.

WebLogic - Patch WebLogic Domain v3

This workflow applies one or more patches to the specified WebLogic 11g or 12c domain. It also supports patching the Java that is used by WebLogic domains.

The workflow uses the Oracle Smart Update (bsu) or OPatch utility to apply the patches. This workflow uses WLST to connect to admin server to stop the Managed Servers and the Admin Server.

Oracle releases WebLogic 11g and 12c patches approximately every five months. The patches can be applied to minor releases or major releases. You must identify which patches are necessary for your domain.

To use this workflow in your environment, see the following information:

Topic	Information Included
"Prerequisites for this Workflow"	List of prerequisites that must be satisfied before you can run this workflow
"How this Workflow Works"	Information about what the workflow does, including validation checks performed, steps executed, and a high-level process flow
"How to Run this Workflow"	Instructions for running this workflow in your environment
"Sample Scenario"	Examples of typical parameter values for this workflow
"Parameters for WebLogic - Patch WebLogic Domain V3" on page 1091	List of input parameters for this workflow

Note: The documentation for this workflow contains steps that are referred to by their base names. The names in the DMA user interface may have a version appended, for example, v2.

Prerequisites for this Workflow

Be sure that the following prerequisites are satisfied before you run the ["WebLogic - Patch WebLogic Domain v3"](#) workflow:

- The latest DMA solution packs require the latest DMA platform. To use the latest solution packs, update the DMA platform. DMA10.50.001.000 solution packs are supported on DMA10.50.001.000 (and later).
- You have installed the Application Server Patching Solution Pack.
- You have provisioned a WebLogic 11g and 12c domain. You can do this by running workflows found in the DMA Application Server Provisioning Solution Pack:
 - Provision Weblogic Software
 - Provision Weblogic Domain and Administration Server
 - Provision Weblogic Managed Servers
 - *Optional:* Provision Weblogic Cluster
 - *Optional:* Increase WebLogic Domain Span
- *Optional:* You have started the following WebLogic 11g and 12c components:
 - Managed Server
 - Administration Server
 - Managed Nodes
- You have an Oracle support contract that enables you to access the appropriate patch ZIP files.
- You have run the WebLogic Discovery workflow and made sure that all metadata is up to date.
- You have verified that the patches to be installed are appropriate for your version of WebLogic 11g or 12c.
- You have added a link to the Java folder and added the link in the **setDomain.sh** file.

For more information about prerequisites for WebLogic 11g and 12c patching, refer to the [WebLogic Product Documentation](#).

How this Workflow Works

The following information describes how the ["WebLogic - Patch WebLogic Domain v3"](#) workflow works:

Overview

The WebLogic - Patch WebLogic Domain workflow first prepares to apply the patch. It determines what user owns the WebLogic 11g or 12c installation. It creates the commands that will be used to execute subsequent steps, gathers and validates the necessary input parameters, and creates additional utility parameters.

The workflow then makes sure that all necessary files exist, have valid specifications, and are in the expected locations. It downloads any required files from the software repository and extracts the contents of the archive files. It collects the patch identifiers from the patch files.

The workflow then prepares the environment. It analyzes the WebLogic domain environment using the DMA REST API to read the metadata for each target. Just before applying the patches, the workflow shuts down or stops the following servers and processes if they are running: the Managed Server (or servers), the Node Manager, and the Administration Server. A server is stopped only if it is local and remote servers of a weblogic domain will not be stopped

Next, the workflow applies the patches. To do this, it utilizes the Oracle Smart Update (bsu) command line utility to apply each of the patches to the specified WebLogic domain. On the Console page, the workflow reports whether each patch succeeded or failed. It collects the patch identifiers of the patches that were successfully installed. Then it updates the WebLogic domain environment using the DMA REST API with the newly retrieved patch identifier metadata.

The workflow ends cleanly. It returns all WebLogic 11g or 12c components to the state they were in when the workflow started. If required, it restarts the WebLogic 11g and 12c Administration Server and the Node Manager, and then starts the WebLogic 11g and 12c Managed Server (or servers).

This workflow also supports patching the Java that is used by WebLogic domains. A symbolic link to the Java parent directory must be provided and specified in the setDomain.sh file. The Java binaries will be extracted in this folder.

Validation Checks Performed

This workflow performs the following validation checks on the input parameters:

Parameter	Validation Checks
BEA Home	The fully qualified paths to the directory must exist.
Patch File List	Checks whether the patch ZIP files exist. If they do not exist, they will be downloaded from the software repository. Multiple files must be separated by commas. Any white space is ignored.
WLS Install Home	The fully qualified path to the directory must exist.

Steps Executed

The WebLogic - Patch WebLogic Domain V3 workflow includes the following steps. Each step must complete successfully before the next step can start. If a step fails, the workflow reports a failure and all subsequent steps are skipped.

Steps Used in WebLogic - Patch WebLogic Domain

Workflow Step	Description
Gather Parameters for WebLogic Patch WebLogic Domain V2	This Step Gathers the minimum required parameter values for Patching a WebLogic Server Installation.
Gather Advanced Parameters for WebLogic Patch WebLogic Domain V3	This Step Gathers the Advanced parameter values for Patching a WebLogic Server Installation.
WebLogic Patching Parameter Validation V4	This step gathers and validates the parameters required to apply patches to a WebLogic 11g or 12c domain.
Check File Download	<p>This step checks for the existence of a file on the target server before downloading that file from the software repository. For each file in the list, this step does the following things:</p> <ol style="list-style-type: none"> 1. Determines whether the file is in the expected location on the target machine. 2. If the file is not in the expected location, adds that file to a list of files that need to be downloaded.
Download Software	This step automates the transfer of files from the HP SA Software Library to individual managed servers for use in downstream workflow steps. Verifies checksum of each file transferred.
WebLogic Extract Patch Files	<p>This step first checks to ensure that the archive file exists. Then, it extracts the archive to the specified directory. Then, it copies the JAR files and XML files to the following directory:</p> <pre>{bea_home}/utils/bsu/cache_dir/{patch_id}</pre>
Cleanup Downloaded Files v2	This step removes all downloaded files and archives.
Gather WebLogic Environment Data V4	This step makes calls via the DMA REST API to obtain structural information about the WebLogic domain.
WebLogic - Stop Servers	This step stops the all the Server associated with a WebLogic Server Installation.
WebLogic Shutdown NodeManager V3	This step stops the Node Manager on the target server if it is running.
WebLogic Verify All Java Processes Stopped	This step validates that all Java processes on a given machine have been stopped.
WebLogic Extract Java Binary Files	This step extracts the Java JDK or JRE file into the Java home of the Weblogic installation.
Restart WebLogic Admin Server V3	This step starts the Admin Server on a given machine or server.

Steps Used in WebLogic - Patch WebLogic Domain, continued

Workflow Step	Description
WebLogic Patch Server V3	This step utilizes the Oracle Smart Update (<i>bsu</i>) command line utility to apply the patches to the specified WebLogic domain.
Restart WebLogic Node Manager V2	This step starts the WebLogic Node Manager on a given machine or server.
Update WebLogic Environment Data V3	This step makes calls via the DMA REST API to get metadata to update the patch names that have been updated.
Restart WebLogic Admin Server V3	This step starts the Admin Server on a give machine or server.
WebLogic Start Managed Server V3	This Steps starts the Managed Servers that were stopped before applying patches, using WLST or StartScripts.
Restart WebLogic Node Manager V2	This step starts the node manager on a given machine or server.
WebLogic Restore Java Binary Files	This step restores the Java Home of the WebLogic installation if the Java patching fails.
Cleanup Downloaded Files v2	This step removes all downloaded files and archives.
WebLogic Start Managed Server V3	This step starts the Managed Servers that were stopped before applying patches, using WLST or StartScripts.
Restart WebLogic Admin Server V3	This step starts the Admin Server on a give machine or server.
Cleanup Downloaded Files v2	This step removes all downloaded files and archives.

For parameter descriptions and defaults, see ["Parameters for WebLogic - Patch WebLogic Domain V3" on page 1091](#).

How to Run this Workflow

The following instructions show you how to customize and run the ["WebLogic - Patch WebLogic Domain v3"](#) workflow in your environment.

The workflow provides default values for some parameters. These default values are usually sufficient for a "typical" installation. You can override the defaults by specifying parameter values in the deployment. Any parameters not explicitly specified in the deployment will have the default values listed in ["Parameters for WebLogic - Patch WebLogic Domain V3"](#) on page 1091.

Note: Before following this procedure, review the ["Prerequisites for this Workflow"](#) on page 1081, and ensure that all requirements are satisfied.

To use the WebLogic - Patch WebLogic Domain V3 workflow:

1. Create a deployable copy of the workflow.
2. Determine the values that you will specify for the following parameters:

Input Parameters for Gather Parameters for WebLogic Patch WebLogic Domain V2

Parameter Name	Default Value	Required	Description
BEA Home	no default	required	Fully qualified path to the product installation directory where the WebLogic 11g or 12c server is installed. For example: /opt/oracle/WebLogic
Patch File List	no default	required	Required: Comma separated list of patches to install.
WLS Install Home	no default	required	Fully qualified path to the home directory that contains the WebLogic 11g or 12c installation . For example: /opt/oracle/WebLogic/wlserver_10.3
WebLogic Staging Location	no default	required	The location where the patch files will be downloaded and extracted, if not found.

Input Parameters for Gather Advanced Parameters for WebLogic Patch WebLogic Domain V3

Parameter Name	Default Value	Required	Description
Call Wrapper	no default	required	The call wrapper for the step. For example, /usr/bin/java
Cleanuup	no default	optional	Specifies if the patch files should be removed after the patch workflow ends.

Input Parameters for Gather Advanced Parameters for WebLogic Patch WebLogic Domain V3, continued

Parameter Name	Default Value	Required	Description
Java JDK File	no default	optional	Name of the Java JDK File, which will be downloaded to the WebLogic Staging Location.
Java JRE File	no default	optional	Name of the Java JRE File, which will be downloaded to the WebLogic Staging Location.
WebLogic User Config File	no default	optional	Used to connect to a WebLogic domain using WLST. If specified, the file path has to be relative to a WebLogic domain path, for example, /connect/userconfigFile. This path will be expanded as /opt/oracle/weblogic/user_projects/domain_temp/connect/userConfigFile and the same value will be used in WLST Connect in multi-domain environment.
WebLogic User Id	no default	optional	WebLogic Admin username for a WebLogic domain. This parameter will be used to connect to WebLogic domain using WLST. The same value will be used in WLST Connect in multi-domain environment.
WebLogic User Password	no default	optional	WebLogic Admin Password for a WebLogic domain. This parameter will be used to connect to WebLogic domain using WLST. The same value will be used in WLST Connect in multi-domain environment.
WebLogic User Key File	no default	optional	Used to connect to a webLogic domain using WLST. If specified, the file path has to be relative to a WebLogic domain path, for example, /connect/userKeyFile. This path will be expanded as /opt/oracle/weblogic/user_projects/domain_temp/connect/userKeyFile and the same value will be used in WLST Connect in multi-domain environment.

Tip: To avoid having to re-enter passwords whenever they change, you can create a policy to provide them to the workflow.

3. Save the changes to the workflow (click **Save** in the lower right corner).
4. Create a new deployment.
5. On the Parameters tab, specify values for the required parameters listed in step 2. You do not need to specify values for those parameters whose default values are appropriate for your environment.
6. On the Targets tab, specify one or more targets for this deployment.

Note: Specify all the targets associated with your WebLogic 11g or 12c domain. The first target specified must be the Administration Server.

7. Save the deployment (click **Save** in the lower right corner).
8. Run the workflow using this deployment.

To verify the results:

The workflow will complete and report SUCCESS on the Console if it has run successfully. If an error occurs during workflow execution, the error is logged, and the workflow terminates in the FAILURE state.

See the Console page output for error messages that indicate whether problems occurred during the application of the patches. Specifically, look at the WebLogic Patch Server step to see the results of applying each individual patch.

Sample Scenario

It is very straightforward to run the WebLogic - Patch WebLogic Domain workflow. This topic shows you typical parameter values to use.

Input Parameters for Gather Parameters for WebLogic Patch WebLogic Domain V2

Parameter Name	Default Value	Required	Description
BEA Home	no default	required	Fully qualified path to the product installation directory where the WebLogic 11g or 12c server is installed. For example: <code>/opt/oracle/WebLogic</code>
Patch File List	no default	required	Required: Comma separated list of patches to install.
WLS Install Home	no default	required	Fully qualified path to the home directory that contains the WebLogic 11g or 12c installation . For example: <code>/opt/oracle/WebLogic/wlserver_10.3</code>
WebLogic Staging Location	no default	required	The location where the patch files will be downloaded and extracted, if not found.

Input Parameters for Gather Advanced Parameters for WebLogic Patch WebLogic Domain V3

Parameter Name	Default Value	Required	Description
Call Wrapper	no default	required	The call wrapper for the step. For example, <code>/usr/bin/java</code>
Cleanuup	no default	optional	Specifies if the patch files should be removed after the patch workflow ends.
Java JDK File	no default	optional	Name of the Java JDK File, which will be downloaded to the WebLogic Staging Location.
Java JRE File	no default	optional	Name of the Java JRE File, which will be downloaded to the WebLogic Staging Location.
WebLogic User Config File	no default	optional	Used to connect to a WebLogic domain using WLST. If specified, the file path has to be relative to a WebLogic domain path, for example, <code>/connect/userconfigFile</code> . This path will be expanded as <code>/opt/oracle/weblogic/user_projects/domain_temp/connect/userconfigFile</code> and the same value will be used in WLST Connect in multi-domain environment.
WebLogic User Id	no default	optional	WebLogic Admin username for a WebLogic domain. This parameter will be used to connect to WebLogic domain using

Input Parameters for Gather Advanced Parameters for WebLogic Patch WebLogic Domain V3, continued

Parameter Name	Default Value	Required	Description
			WLST. The same value will be used in WLST Connect in multi-domain environment.
WebLogic User Password	no default	optional	WebLogic Admin Password for a WebLogic domain. This parameter will be used to connect to WebLogic domain using WLST. The same value will be used in WLST Connect in multi-domain environment.
WebLogic User Key File	no default	optional	Used to connect to a webLogic domain using WLST. If specified, the file path has to be relative to a WebLogic domain path, for example, /connect/userKeyFile. This path will be expanded as /opt/oracle/weblogic/user_projects/domain_temp/connect/userKeyFile and the same value will be used in WLST Connect in multi-domain environment.

Parameters for WebLogic - Patch WebLogic Domain V3

The following tables describe the required and optional input parameters for this workflow.

Parameters defined in this step: Gather Parameters for WebLogic Patch WebLogic Domain V2

Parameter Name	Default Value	Required	Description
BEA Home	no default	required	Fully qualified path to the product installation directory where the WebLogic 11g or 12c server is installed. For example: <code>/opt/oracle/WebLogic</code>
Patch File List	no default	required	Required: Comma separated list of patches to install.
WLS Install Home	no default	required	Fully qualified path to the home directory that contains the WebLogic 11g or 12c installation . For example: <code>/opt/oracle/WebLogic/wlserver_10.3</code>
WebLogic Staging Location	no default	required	The location where the patch files will be downloaded and extracted, if not found.

Parameters defined in this step: Gather Advanced Parameters for WebLogic Patch WebLogic Domain V3

Parameter Name	Default Value	Required	Description
Call Wrapper	no default	required	The call wrapper for the step. For example, <code>/usr/bin/java</code>
Cleanup	no default	optional	Specifies if the patch files should be removed after the patch workflow ends.
Java JDK File	no default	optional	Name of the Java JDK File, which will be downloaded to the WebLogic Staging Location.
Java JRE File	no default	optional	Name of the Java JRE File, which will be downloaded to the WebLogic Staging Location.
WebLogic User Config File	no default	optional	Used to connect to a WebLogic domain using WLST. If specified, the file path has to be relative to a WebLogic domain path, for example, <code>/connect/userconfigFile</code> . This path will be expanded as <code>/opt/oracle/weblogic/user_projects/domain_temp/connect/userConfigFile</code> and the same value will be used in WLST Connect in multi-domain environment.
WebLogic User Id	no default	optional	WebLogic Admin username for a WebLogic domain. This parameter will be used to connect to WebLogic domain using WLST. The same value will be used in WLST Connect in multi-domain environment.
WebLogic	no	optional	WebLogic Admin Password for a WebLogic domain. This

Parameters defined in this step: Gather Advanced Parameters for WebLogic Patch WebLogic Domain V3, continued

Parameter Name	Default Value	Required	Description
User Password	default		parameter will be used to connect to WebLogic domain using WLST. The same value will be used in WLST Connect in multi-domain environment.
WebLogic User Key File	no default	optional	Used to connect to a webLogic domain using WLST. If specified, the file path has to be relative to a WebLogic domain path, for example, /connect/userKeyFile. This path will be expanded as /opt/oracle/weblogic/user_projects/domain_temp/connect/userKeyFile and the same value will be used in WLST Connect in multi-domain environment.

WebLogic - Rollback Patch

This workflow removes patch from the specified WebLogic domain.

The workflow uses the Oracle Smart Update (bsu) or OPatch utility to remove the patches.

To use this workflow in your environment, see the following information:

Topic	Information Included
"Prerequisites for this Workflow"	List of prerequisites that must be satisfied before you can run this workflow
"How this Workflow Works"	Information about what the workflow does, including validation checks performed, steps executed, and a high-level process flow
"How to Run this Workflow"	Instructions for running this workflow in your environment
"Sample Scenario"	Examples of typical parameter values for this workflow
Parameters	List of input parameters for this workflow

Note: The documentation for this workflow contains steps that are referred to by their base names. The names in the HPE DMA user interface may have a version appended, for example, v2.

Prerequisites for this Workflow

Be sure that the following prerequisites are satisfied before you run the WebLogic - Rollback Patch workflow:

- This solution requires DMA version 10.40 (or later).

The latest DMA solution packs require the latest DMA platform. To use the latest solution packs, update the DMA platform. DMA 10.40 solution packs are supported on DMA 10.40 (and later).
- You have installed the DMA Application Server Patching Solution Pack.
- You have provisioned a WebLogic domain. You can do this by running workflows found in the DMA Application Server Provisioning Solution Pack:
 - Provision Weblogic Software
 - Provision Weblogic Domain and Administration Server
 - Provision Weblogic Managed Servers
 - *Optional:* Provision Weblogic Cluster
 - *Optional:* Increase WebLogic Domain Span
- *Optional:* You have started the following WebLogic components:
 - Managed Server
 - Administration Server
 - Managed Nodes
- You have an Oracle support contract that enables you to access the appropriate patch ZIP files.
- You have run the WebLogic Discovery workflow and made sure that all metadata is up to date.
- You have verified that the patches to be installed are appropriate for your version of WebLogic.

For more information about prerequisites for WebLogic patching, refer to the [WebLogic Product Documentation](#).

How this Workflow Works

The following information describes how the WebLogic - Rollback Patch workflow works:

Overview

The WebLogic - Rollback Patch workflow first prepares to rollback the patch. It determines what user owns the WebLogic installation. It creates the commands that will be used to execute subsequent steps, gathers and validates the necessary input parameters, and creates additional utility parameters.

The workflow then makes sure that all necessary files exist, have valid specifications, and are in the expected locations. It downloads any required files from the software repository and extracts the contents of the archive files.

The workflow then prepares the environment. It analyzes the WebLogic domain environment using the DMA REST API to read the metadata for each target. Just before removing the patches, the workflow shuts down or stops the following servers and processes if they are running: the Managed Server (or servers), the Node Manager, and the Administration Server.

Next, the workflow removes the patches. On the console page, the workflow reports whether rollback of patch succeeded or failed.

The workflow ends cleanly. It returns all WebLogic components to the state they were in when the workflow started. If required, it restarts the WebLogic Administration Server and the Node Manager, and then starts the WebLogic Managed Server (or servers).

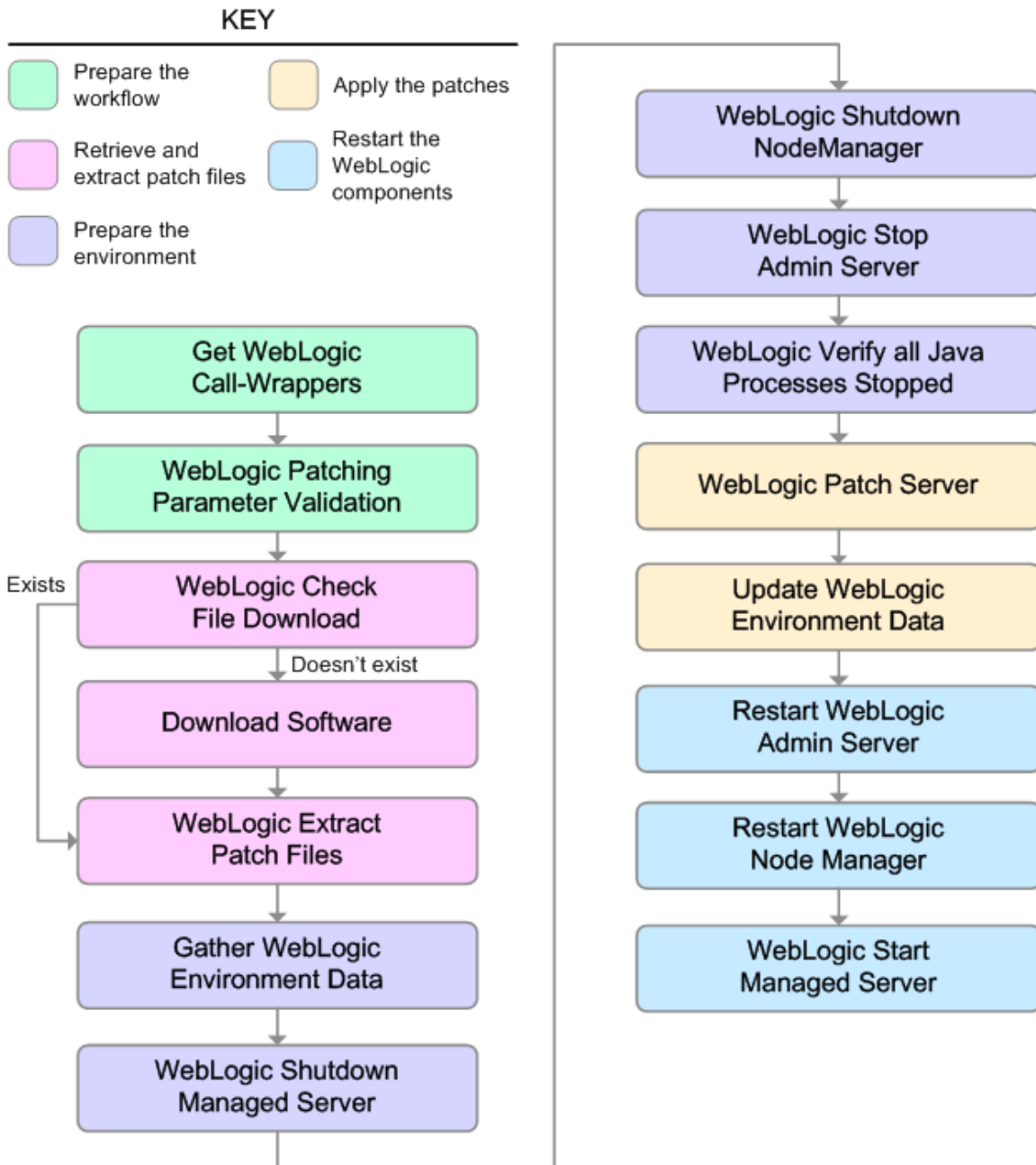
Validation Checks Performed

This workflow performs the following validation checks on the input parameters:

Parameter	Validation Checks
BEA Home WLS Install Home	The fully qualified paths to the directories must exist.
Patch Rollback List	The patch workflow checks if this patch ID is applied to the given WLS home installation. If False, then the workflow will fail.
WebLogic User Config File / Weblogic User Key File	The pair must exist (although optional , these values must exist as a pair).
WebLogic User Id WebLogic User Password	The pair must exist (although optional , these values must exist as a pair).

Steps Executed

The WebLogic - Rollback Patch WebLogic Domain workflow includes the following steps. Each step must complete successfully before the next step can start. If a step fails, the workflow reports a failure and all subsequent steps are skipped.



Steps Used in WebLogic - Patch WebLogic Domain

Workflow Step	Description
Gather Parameters for WebLogic Rollback Patch	This step determines what user owns the installation and creates the commands that will be used by the workflow to run subsequent steps. It also sets up some parameters that are used to specify an empty string, a True value, and a False value for input parameters of subsequent steps.
Gather Advanced Parameters for WebLogic Rollback Patch	This step gathers the advanced parameter values for patching a WebLogic server installation.
WebLogic Patching Parameter Validation	This step prepares the parameters needed to apply patches to a WebLogic domain.
Gather WebLogic Environment Data v3	This step makes calls via the DMA REST API to obtain structural information about the WebLogic domain.
WebLogic: Stop Servers	This step stops the all the servers associated with a WebLogic server installation. Stops the managed servers that are local to the machine using WebLogic Scripting Tool (WLST) by connecting to the admin server. Stops the admin server if the admin server is local to the machine.
WebLogic Shutdown NodeManager V3	This step stops the Node Manager on a given machine or server.
WebLogic Verify All Java Processes Stopped	This step validates that all running Java processes on the target server that are associated with the WebLogic server have been stopped.
WebLogic Rollback Patch	This step utilizes the BEA Smart Update (bsu) command line utility or OPatch utility to remove the patches from a given WebLogic domain.
Restart WebLogic Admin Server V3	This step starts the WebLogic Administration Server on a give machine or server.
Update WebLogic Environment Data V3	This step makes calls via the DMA REST API to get metadata to update the patches names that have been updated.
Restart WebLogic Admin Server V3	This step starts the WebLogic Administration Server on a give machine or server.
Restart WebLogic Node Manager V2	This step starts the WebLogic Node Manager on a given machine or server.

Steps Used in WebLogic - Patch WebLogic Domain, continued

Workflow Step	Description
WebLogic Start Managed Server V3	This step starts the managed servers that were stopped before applying patches. Starts the managed servers using WLST or StartScripts.

For parameter descriptions and defaults, see ["Parameters for WebLogic - Rollback Patch"](#).

How to Run this Workflow

The following instructions show you how to customize and run the WebLogic - Rollback Patch workflow in your environment.

The workflow provides default values for some parameters. These default values are usually sufficient for a "typical" installation. You can override the defaults by specifying parameter values in the deployment. Any parameters not explicitly specified in the deployment will have the default values listed in ["Parameters for WebLogic - Rollback Patch"](#).

Note: Before following this procedure, review the ["Prerequisites for this Workflow"](#) on page 1094, and ensure that all requirements are satisfied.

To use the WebLogic - Patch WebLogic Domain workflow:

1. Create a deployable copy of the workflow.
2. Determine the values that you will specify for the following parameters:

Input Parameters for Gather Parameters for WebLogic Patch WebLogic Domain V2

Parameter Name	Default Value	Required	Description
BEA Home	no default	required	Fully qualified path to the product installation directory where the WebLogic server is installed. For example: <code>/opt/oracle/WebLogic</code>
Patch File List	no default	required	Comma separated list of patches to install. For example: <code>/opt/wlpatch/pl4154043_1035_Generic.zip</code>
WLS Install Home	no default	required	Fully qualified path to the home directory that contains the WebLogic installation . For example: <code>/opt/oracle/WebLogic/wlserver_10.3</code>
WebLogic Staging Location	no default	required	This is the location where the patch files will be downloaded if not found and extracted

Input Parameters for Gather Advanced Parameters for WebLogic Patch WebLogic Domain V2

Parameter Name	Default Value	Required	Description
Call Wrapper	no default	required	Fully qualified path to the product installation directory where the WebLogic server is installed. For example: <code>/opt/oracle/WebLogic</code>
Cleanup	no	optional	Specifies if the patch files should be removed after the

Input Parameters for Gather Advanced Parameters for WebLogic Patch WebLogic Domain V2, continued

Parameter Name	Default Value	Required	Description
	default		patch workflow ends.
WebLogic User Config File	no default	optional	<p>This parameter will be used to connect to a webLogic domain using WLST. If Specified, the file path has to be relative to a WebLogic domain path. For example:</p> <p>/connect/userconfigFile will be expanded as /opt/oracle/weblogic/user_projects/domain_temp/connect/userConfigFile</p> <p>The same value will be used in WLST Connect in multi domain environment.</p>
WebLogic User Id	no default	optional	<p>The WebLogic admin username for the a WebLogic domain. This parameter will be used to connect to WebLogic domain using WLST. The same value will be used in WLST Connect in multi-domain environment.</p>
WebLogic User Password	no default	optional	<p>The WebLogic admin password for the a WebLogic domain. This parameter will be used to connect to WebLogic domain using WLST.</p> <p>The same value will be used in WLST Connect in multi-domain environment.</p>
Weblogic User Key File	no default	optional	<p>This parameter will be used to connect to a WebLogic domain using WLST. If specified, the file path has to be relative to a WebLogic domain path. For example:</p> <p>/connect/userKeyFile will be expanded as /opt/oracle/weblogic/user_projects/domain_temp/connect/userKeyFile</p> <p>The same value will be used in WLST Connect in multi-domain environment.</p>

Tip: To avoid having to re-enter passwords whenever they change, you can create a policy to provide them to the workflow.

Note: This is the minimum set of parameters required to run this workflow. You may need to expose additional parameters depending on your patching objectives.

See "[Parameters for WebLogic - Rollback Patch](#)" for detailed descriptions of all input parameters for this workflow, including default values.

- In the workflow editor, expose any additional parameters that you need. You will specify values for those parameters when you create the deployment.
- Save the changes to the workflow (click **Save** in the lower right corner).

5. Create a new deployment.
6. On the Parameters tab, specify values for the required parameters listed in step 2. You do not need to specify values for those parameters whose default values are appropriate for your environment.
7. On the Targets tab, specify one or more targets for this deployment.

Note: Specify all the targets associated with your WebLogic domain. The first target specified must be the Administration Server.

8. Save the deployment (click **Save** in the lower right corner).
9. Run the workflow using this deployment.

To verify the results:

The workflow will complete and report SUCCESS on the Console if it has run successfully. If an error occurs during workflow execution, the error is logged, and the workflow terminates in the FAILURE state.

See the Console page output for error messages that indicate whether problems occurred during the application of the patches. Specifically, look at the WebLogic Patch Server step to see the results of applying each individual patch.

Sample Scenario

It is very straightforward to run the WebLogic - Patch WebLogic Domain workflow. This topic shows you typical parameter values to use.

Input Parameters for Gather Parameters for WebLogic Rollback Patch

Parameter Name	Example Value	Description
BEA Home	see description	Fully qualified path to the product installation directory where the WebLogic server is installed. For example: <code>/opt/oracle/WebLogic</code>
Patch Rollback List	see description	Comma separated list of patches to be removed . For example: <code>UH52,8PE3</code>
WLS Install Home	see description	Fully qualified path to the home directory that contains the WebLogic installation . For example: <code>/opt/oracle/WebLogic/wlserver_10.3</code>
WebLogic Staging Location	see description	This is the location where the patch files will be downloaded if not found and extracted

Input Parameters for Gather Advanced Parameters for WebLogic Rollback Patch

Parameter Name	Example Value	Description
Call Wrapper	see description	Fully qualified path to the product installation directory where the WebLogic server is installed. For example: <code>/opt/oracle/WebLogic</code>
Cleanup	see description	Specifies if the patch files should be removed after the patch workflow ends.
WebLogic User Config File	see description	This parameter will be used to connect to a webLogic domain using WLST. If Specified, the file path has to be relative to a WebLogic domain path. For example: <code>/connect/userconfigFile</code> will be expanded as <code>/opt/oracle/weblogic/user_projects/domain_temp/connect/userConfigFile</code> The same value will be used in WLST Connect in multi domain environment.
WebLogic User Id	see description	The WebLogic admin username for the a WebLogic domain. This parameter will be used to connect to WebLogic domain using WLST. The same value will be used in WLST Connect in multi-domain environment.
WebLogic User Password	see description	The WebLogic admin password for the a WebLogic domain. This parameter will be used to connect to WebLogic domain using WLST. The same value will be used in WLST Connect in multi-domain environment.

Input Parameters for Gather Advanced Parameters for WebLogic Rollback Patch, continued

Parameter Name	Example Value	Description
Weblogic User Key File	see description	<p>This parameter will be used to connect to a WebLogic domain using WLST. If specified, the file path has to be relative to a WebLogic domain path. For example:</p> <pre>/connect/userKeyFile will be expanded as /opt/oracle/weblogic/user_projects/domain_ temp/connect/userKeyFile</pre> <p>The same value will be used in WLST Connect in multi-domain environment.</p>

Parameters for WebLogic - Rollback Patch

The following tables describe the required and optional input parameters for this workflow.

Parameters Defined in this Step: Gather Parameters for WebLogic Rollback Patch

Parameter Name	Default Value	Required	Description
BEA Home	no default	required	Fully qualified path to the product installation directory where the WebLogic server is installed. For example: /opt/oracle/WebLogic
Patch Rollback List	no default	required	Comma separated list of patches to be removed . For example: UH52,8PE3
WLS Install Home	no default	required	Fully qualified path to the home directory that contains the WebLogic installation . For example: /opt/oracle/WebLogic/wlserver_10.3
WebLogic Staging Location	no default	required	This is the location where the patch files will be downloaded if not found and extracted

Additional Parameters Defined in this Step: Gather Advanced Parameters for WebLogic Rollback Patch

Parameter Name	Default Value	Required	Description
Call Wrapper	no default	required	Fully qualified path to the product installation directory where the WebLogic server is installed. For example: /opt/oracle/WebLogic
Cleanup	no default	optional	Specifies if the patch files should be removed after the patch workflow ends.
WebLogic User Config File	no default	optional	This parameter will be used to connect to a webLogic domain using WLST. If Specified, the file path has to be relative to a WebLogic domain path. For example: /connect/userconfigFile will be expanded as /opt/oracle/weblogic/user_projects/domain_temp/connect/userConfigFile The same value will be used in WLST Connect in multi domain environment.
WebLogic User Id	no default	optional	The WebLogic admin username for the a WebLogic domain. This parameter will be used to connect to WebLogic domain using WLST. The same value will be used in WLST Connect in multi-domain environment.
WebLogic User Password	no default	optional	The WebLogic admin password for the a WebLogic domain. This parameter will be used to connect to WebLogic domain using WLST. The same value will be used in WLST Connect in multi-domain environment.

Additional Parameters Defined in this Step: Gather Advanced Parameters for WebLogic Roll-back Patch, continued

Parameter Name	Default Value	Required	Description
Weblogic User Key File	no default	optional	<p>This parameter will be used to connect to a WebLogic domain using WLST. If specified, the file path has to be relative to a WebLogic domain path. For example:</p> <p><code>/connect/userKeyFile</code> will be expanded as <code>/opt/oracle/weblogic/user_projects/domain_temp/connect/userKeyFile</code></p> <p>The same value will be used in WLST Connect in multi-domain environment.</p>

IBM WebSphere

This section includes the following topics:

Workflow type	Workflow name
Provisioning	"Provision WebSphere and Custom Node" on the next page
	"Provision WebSphere Custom Node Profile From Existing Install" on page 1124
	" Provision WebSphere and Deployment Manager" on page 1138
	"Provision WebSphere and Stand-Alone" on page 1156
	"Provision WebSphere Stand-Alone Profile From Existing Install" on page 1173
	"WebSphere - Provision IBM HTTP Server" on page 1187
	"Provision WebSphere 7 and Custom Node" on page 1209
	"Provision WebSphere 7 and Deployment Manager" on page 1225
	"Provision WebSphere 7 StandAlone Profile" on page 1241
	"Provision IBM HTTP Server 7 and Plug-In" on page 1256
	"Create Custom Node from Existing WebSphere 7 Install" on page 1289
	"Create StandAlone from Existing WebSphere 7 Install" on page 1274
	"WebSphere - Provision WebSphere SDK Java" on page 1393
Patching	"WebSphere 8 - Patch Network Cell" on page 1374
	"IBM HTTP Server - Patch Software v2" on page 1383
	WebSphere - Patching Master Flow
	WebSphere - Uninstall WebSphere SDK
Configuring	"Create and Configure WebSphere Data Sources" on page 1303
	"Create and Configure WebSphere Web Server Definitions" on page 1325
	"Configure WebSphere Cluster and Cluster Members" on page 1403
Release Management	"WebSphere - Code Release" on page 1339
	"WebSphere - Code Release on Cluster" on page 1359

Provision WebSphere and Custom Node

Use this workflow to install the WebSphere 8.0 or 8.5.x Base core binaries and, optionally, create a custom profile.

A custom profile initially contains an empty node with no servers. The workflow can add (federate) the server to the pertinent cell when the profile is created, or you can add it later yourself.

To use this workflow in your environment, see the following information:

Topic	Information Included
"Prerequisites for this Workflow"	List of prerequisites that must be satisfied before you can run this workflow
"How this Workflow Works"	Information about what the workflow does, including validation checks performed, steps executed, and a high-level process flow
"How to Run this Workflow"	Instructions for running this workflow in your environment
"Sample Scenario"	Examples of typical parameter values for this workflow
Parameters	List of input parameters for this workflow

Note: The documentation for this workflow contains steps that are referred to by their base names. The names in the DMA user interface may have a version appended, for example, v2.

Prerequisites for this Workflow

Be sure that the following prerequisites are satisfied before you run the Provision WebSphere and Custom Node workflow:

1. This workflow requires unchallenged `sudo` access to a user (typically `root`) who can access all required files and directories.
2. Per the IBM WebSphere 8 documentation, the following system libraries are required before provisioning WebSphere 8.0 or 8.5.x on 64-bit and 32-bit Red Hat Linux targets:

Platform	Required Library
64-bit Red Hat Enterprise Linux version 5	compat-libstdc++-33-3.2.3-61 compat-db-4.2.52-5.1 gtk2-2.10.4-29.el5 gtk2-engines-2.8.0-3.el5 ksh-20080202-14 libXp-1.0.0-8 libXmu-1.0.2-5 libXtst-1.0.1-3.1 pam-0.99.6.2-3.26.el5 elfutils-0.125-3.el5 elfutils-libs-0.125-3.el5 libXft-2.1.10-1.1 libstdc++-4.1.2-48 <div> If the target server supports both 32-bit and 64-bit applications then both the 32-bit and 64-bit versions of the following libraries are required: </div> compat-libstdc++-33-3.2.3-61 compat-db-4.2.52-5.1 gtk2-2.18.9-4 gtk2-engines-2.18.4-5 libstdc++-4.1.2-48 libXft-2.1.10-1.1 libXp-1.0.0-8 libXmu-1.0.2-5 libXtst-1.0.1-3.1 pam-0.99.6.2-3.26.el5
64-bit Red Hat Enterprise Linux version 6	compat-libstdc++-33-3.2.3-69 compat-db-4.6.21-15 ksh-20100621-2 gtk2-2.18.9-4 gtk2-engines-2.18.4-5 libXp-1.0.0-15.1 libXmu-1.0.5-1 libXtst-1.0.99.2-3 pam-1.1.1-4 elfutils-0.148-1

Platform	Required Library
	<p>elfutils-libs-0.148-1 libXft-2.1.13-4.1 libstdc++-4.4.4-13</p> <p>If the target server supports both 32-bit and 64-bit applications then both the 32-bit and 64-bit versions of the following libraries are required:</p> <p>compat-libstdc++-33-3.2.3-69 compat-db-4.6.21-15 libstdc++-4.4.4-13 libXp-1.0.0-15.1 libXmu-1.0.5-1 libXtst-1.0.99.2-3 pam-1.1.1-4 libXft-2.1.13-4.1 gtk2-2.18.9-4 gtk2-engines-2.18.4-5</p>

Make sure that these libraries exist on each target server before running this workflow. If newer versions of these libraries are available, you can install the newer versions.

3. This workflow will install WebSphere Application Server as root because of the following IBM documented limitations:
 - Creation of a Linux service for WebSphere Application Server
 - Native registration with the operating system
 - Port conflicts that may occur with other installations of WebSphere Application Server that are not registered with the operating system

If there is a need to run as a non-root user after installation, you can run a recursive `chown` under the installation root and set owner permissions accordingly.

For more information about prerequisites for WebSphere 8, refer to the [WebSphere 8 Product Documentation](#).

How this Workflow Works

This topic contains the following information about the ["Provision WebSphere and Custom Node"](#) workflow:

Overview

This workflow does the following three things in the order shown:

1. Installs the IBM Install Manager
2. Installs WebSphere Network Deployment version 8.0 or 8.5.x
3. Creates a Custom Node profile

The workflow checks to see if the WebSphere 8.0 or 8.5.x binary archive files exist on the target machine. If they do not, the files are downloaded from the software repository.

See the following topics for detailed information:

[Validation Checks Performed](#)

[Steps in this Workflow](#)

[Process Flow](#)

Note: This workflow has been updated to account for the significant changes in the way that WebSphere 8 are installed.

Validation Checks Performed

Most of the validation centers on special characters and spaces in the parameters. There are also validation checks that happen at the operating system level, including file system space checks and RPM checks (on Red Hat Linux platforms only).

The workflow first performs the following parameter checks:

1. Required parameters have values specified.
2. WebSphere specific names do not contain the following characters: `/ \ * , ; = + ? | < > & % ' " [] # $ ^ { }`
3. Parameters do not contain illegal characters for the parameter type.
4. Flag parameters are set to true or false.
5. Integer parameters are set to appropriate integer values.
6. Mutually dependent parameters are specified appropriately as a set.
7. Parameters are set to one of the values if the parameter has a list of valid values.
8. License Acceptance is true (for workflows that input the License Acceptance parameter).
9. All specified file names are legal file names.
10. All specified locations are legal path names. If they do not exist they will be created.

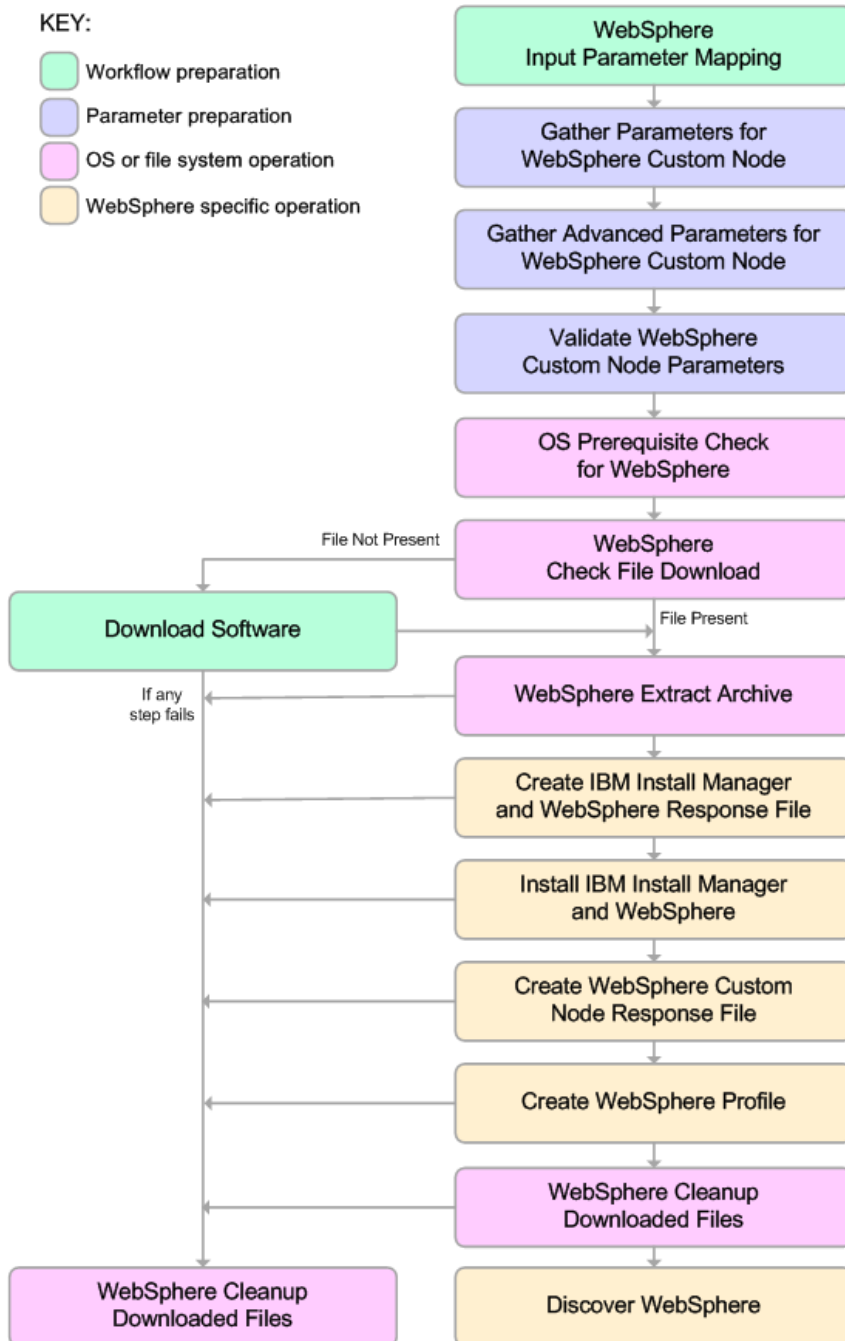
Note: For more information about valid parameter values, see ["Parameters for Provision WebSphere and Custom Node"](#).

The workflow then performs the following operating system checks on the target machine:

1. All required libraries are present (see ["Prerequisites for this Workflow"](#)).
2. Sufficient disk space is available to install WebSphere 8.0 or 8.5.x.
3. Sufficient disk space is available to extract the binary files from the compressed archive.

Steps Executed

The Provision WebSphere and Custom Node workflow includes the following steps. Each step must complete successfully before the next step can start. If a step fails, the workflow reports a failure, and all subsequent steps are skipped.



Process Flow

This workflow performs the following tasks:

1. Creates the call wrapper and determines the target server platform type.
2. Gathers and validates the parameters needed to install Provision WebSphere and Custom Node and create a Custom Node profile (see ["Validation Checks Performed " on page 1111](#)).
3. Checks the following:
 - a. Documented library requirements for WebSphere 8 (see the ["Prerequisites for this Workflow"](#)).
 - b. File system space requirements where WebSphere 8.0 or 8.5.x will be installed.
 - c. Temporary space requirements where the compressed software will be extracted before it is installed.
4. Determines whether the WebSphere 8.0 or 8.5.x binary archive is present on the target machine. If the archive is not present, the workflow downloads it from the software repository.
5. Extracts the WebSphere 8.0 or 8.5.x binary archive to the specified directory.
6. Creates a response file for the purpose of installing a new instance of WebSphere 8.0 or 8.5.x.
7. Installs the IBM Installation Manager and a new WebSphere 8.0 or 8.5.x instance on the target server.
8. Creates a new response file for the purpose of creating a Custom Node profile on top of the WebSphere 8.0 or 8.5.x installation.
9. Creates a custom profile on top of the WebSphere 8.0 or 8.5.x installation.
10. Cleans up any files that were downloaded—for either workflow success or failure.

Note: The parameters Cleanup on Success and Cleanup on Failure are defaulted to True. If they are set to False, the downloaded files are not cleaned up.

11. Discovers any WebSphere 8.0 or 8.5.x cells, clusters, and managed servers associated with the Profile Root that you specify. If these items are found, they are added to the DMA environment.

How to Run this Workflow

The following instructions show you how to customize and run the ["Provision WebSphere and Custom Node"](#) workflow in your environment.

The workflow provides default values for some parameters. These default values are usually sufficient for a "typical" installation. You can override the defaults by specifying parameter values in the deployment. You can also expose additional parameters in the workflow, if necessary, to accomplish more advanced scenarios. Any parameters not explicitly specified in the deployment will have the default values listed in ["Parameters for Provision WebSphere and Custom Node"](#).

Note: Before following this procedure, review the ["Prerequisites for this Workflow"](#), and ensure that all requirements are satisfied.

To use the Provision WebSphere and Custom Node workflow:

1. Create a deployable copy of the workflow.
2. Determine the values that you will specify for the following parameters:

Parameters Defined in this Step: Gather Parameters for WebSphere Custom Node

Parameter Name	Default Value	Required	Description
Cell Name	no default	required	Unique cell name that does not contain any of the following special characters <code>/ \ * , ; = + ? < > & % ' " [] # \$ ^ { }</code> . If you plan to federate into an existing cell later, make sure that this name is not the same as the existing cell name.
Dmgr Admin Password	no default	optional	Administrative user password for the Deployment Manager. When Enable Security is set to true, this parameter must contain a string that does not begin with a dash(-) or contain a space().
Dmgr Admin User	no default	optional	Deployment Manager administrative user. When Enable Security is set to true, this parameter must contain a string that does not begin with a dash(-), a period(.), or a space(). It cannot contain any of the following characters <code>/ \ * , ; = + ? < > & % ' " [] # \$ ^ { }</code> .
Dmgr HostName	no default	optional	Host name or IP address of the machine where the Deployment Manager is running. Specify this parameter and the Dmgr Port parameter to federate the new custom node as it is created. If you do not specify a value for this parameter, the new custom node is not federated (you must federate it later). Required if Federate Later is set to false.
Dmgr Port	no default	optional	The SOAP port on which the Deployment Manager is

Parameters Defined in this Step: Gather Parameters for WebSphere Custom Node, continued

Parameter Name	Default Value	Required	Description
			listening. Specify this parameter and the Dmgr Host Name parameter to federate the new custom node as it is created. If you do not specify a value for this parameter, the new custom node is not federated (you must federate it later). Required if Federate Later is set to false.
Enable Security	no default	required	Enables administrative security on the Deployment Manager. Must be set to either true or false. If Enable Security is true, the Dmgr Admin User and Dmgr Admin Password parameters must have values.
Federate Later	no default	required	If false, the new custom node will be federated by the workflow during profile creation; you must specify Dmgr HostName and Dmgr Port to do this. If true, you must federate it later manually by using the addNode command.
Install Manager Binary Download Location	/opt/IBM/iim	required	Fully qualified path to where the compressed Install Manager software package will be downloaded on the target machine. For example: /opt/IBM/iim
Install Manager Binary Files	no default	required	Name of the compressed Install Manager software package.
Install Manager Extract Location	no default	required	Fully qualified path where the compressed software will be extracted on the target machine. This location cannot be the same as WebSphere Extract Location.
Install Manager Install Location	no default	required	Fully qualified path where Install Manager will be installed. For example: /opt/IBM/InstallManager
License Acceptance	false	required	Acknowledges that the end user agrees to the IBM International Program License Agreement. This is set to false by default and must be set to true in order for the installation to continue.
Node Name	no default	required	Unique node name that cannot contain any of the following special characters / \ * , ; = + ? < > & % ' " [] # \$ ^ { }. If you plan to federate into an existing cell later, make sure that the name is unique within that cell.
Profile Name	no default	required	A unique profile name. It cannot begin with a period (.) and cannot contain any of the following special characters / \ * , ; = + ? < > & % ' " [] # \$ ^ { }.

Parameters Defined in this Step: Gather Parameters for WebSphere Custom Node, continued

Parameter Name	Default Value	Required	Description
Web Service Password	no default	required	Password for the discovery web service API.
Web Service User	no default	required	User capable of modifying the managed environment through the discovery web service API.
WebSphere Binary Download Location	/opt/IBM/WAS	required	Fully qualified path to the compressed WebSphere software package on the target machine.
WebSphere Binary Files	no default	required	Comma separated list of file names of the compressed WebSphere software packages.
WebSphere Extract Location	no default	required	Fully qualified path where the compressed software will be extracted on the target machine. This location cannot be the same as Install Manager Extract Location.
WebSphere Install Location	no default	required	Fully qualified path where WebSphere will be installed.
Windows Administrator Password	no default	required	The Windows Administrator password. Required for Windows.
Windows Administrator User	no default	required	This is the Windows Administrator user. Required for Windows.

Note: This is the minimum set of parameters required to run this workflow. You may need to expose additional parameters depending on your provisioning objectives.

See ["Parameters for Provision WebSphere and Custom Node"](#) for detailed descriptions of all input parameters for this workflow, including default values.

Tip: To avoid having to re-enter passwords whenever they change, you can create a policy to provide them to the workflow

3. In the workflow editor, expose any additional parameters that you need. You will specify values for those parameters when you create the deployment.
4. Save the changes to the workflow (click **Save** in the lower right corner).
5. Create a new deployment.
6. On the Parameters tab, specify values for the required parameters listed in step 2 and any

additional parameters that you have exposed. You do not need to specify values for those parameters whose default values are appropriate for your environment.

7. On the Targets tab, specify one or more targets for this deployment.
8. Save the deployment (click **Save** in the lower right corner).
9. Run the workflow using this deployment.

To verify the results:

The workflow will complete and report SUCCESS on the Console if it has run successfully. If an error occurs during workflow execution, the error is logged, and the workflow terminates in the FAILURE state.

Be sure to also perform the following steps:

1. After the workflow has completed, run the following command to check the version of WebSphere Application Server that was installed:

```
WAS_ROOT/bin/versionInfo.sh
```

Here, *WAS_ROOT* is the directory where WebSphere 8.0 or 8.5.x is installed. This is the path that you specified in the WebSphere Install Location parameter.

2. Validate that the profile has been created and is running by doing the following:
 - a. View the *WAS_ROOT*/profiles/*PROFILE_NAME*/logs/AboutThisProfile.txt file. This file is created after the creation of the profile and contains specific information about the profile.

Here, *PROFILE_NAME* is the name of the profile that you just created. This is the name that you specified in the Profile Name parameter.

- b. Change to the *WAS_ROOT*/profiles/*PROFILE_NAME*/logs/*CELL_NAME* directory, and tail the SystemOut.log file. Look for the following line:

```
Server CELL_NAME open for e-business
```

Here, *CELL_NAME* is the name of the WebSphere 8.0 or 8.5.x cell to which this profile pertains. This is the name that you specified in the Cell Name parameter.

Sample Scenario

This topic shows you typical parameter values used for the ["Provision WebSphere and Custom Node"](#) workflow.

Tip: To avoid having to re-enter passwords whenever they change, you can create a policy to provide them to the workflow.

New Install with Custom Node Profile – Parameter Value Examples

Parameter Name	Example Value	Description
Cell Name	Dev NodeCell	Unique cell name that does not contain any of the following special characters / \ * , ; = + ? < > & % ' " [] # \$ ^ { }. If you plan to federate into an existing cell later, make sure that this name is not the same as the existing cell name.
Dmgr Admin Password	wasPassWord	Administrative user password for the Deployment Manager. When Enable Security is set to true, this parameter must contain a string that does not begin with a dash(-) or contain a space().
Dmgr Admin User	wasadmin	Deployment Manager administrative user. When Enable Security is set to true, this parameter must contain a string that does not begin with a dash(-), a period(.), or a space(). It cannot contain any of the following characters / \ * , ; = + ? < > & % ' " [] # \$ ^ { }.
Dmgr HostName		Host name or IP address of the machine where the Deployment Manager is running. Specify this parameter and the Dmgr Port parameter to federate the new custom node as it is created. If you do not specify a value for this parameter, the new custom node is not federated (you must federate it later). Required if Federate Later is set to false.
Dmgr Port		The SOAP port on which the Deployment Manager is listening. Specify this parameter and the Dmgr Host Name parameter to federate the new custom node as it is created. If you do not specify a value for this parameter, the new custom node is not federated (you must federate it later). Required if Federate Later is set to false.
Enable Security	true	Enables administrative security on the Deployment Manager. Must be set to either true or false. If Enable Security is true, the Dmgr Admin User and Dmgr Admin Password parameters must have values.
Federate Later	true	If false, the new custom node will be federated by the workflow during profile creation; you must specify Dmgr HostName and Dmgr Port to do this. If true, you must federate it later manually by using the addNode command.
Install Manager Binary Download Location	/opt/IBM/iim	Fully qualified path to where the compressed Install Manager software package will be downloaded on the target machine. For example: /opt/IBM/iim

New Install with Custom Node Profile – Parameter Value Examples, continued

Parameter Name	Example Value	Description
Install Manager Binary Files	IBM_Install_Manager_Linux.zip	Name of the compressed Install Manager software package.
Install Manager Extract Location	/opt/IBM/iim	Fully qualified path where the compressed software will be extracted on the target machine. This location cannot be the same as WebSphere Extract Location.
Install Manager Install Location	/opt/IBM/installManager	Fully qualified path where Install Manager will be installed. For example: /opt/IBM/InstallManager
License Acceptance	true	Acknowledges that the end user agrees to the IBM International Program License Agreement. This is set to false by default and must be set to true in order for the installation to continue.
Node Name	DevNode	Unique node name that cannot contain any of the following special characters / \ * , ; = + ? < > & % ' " [] # \$ ^ { }. If you plan to federate into an existing cell later, make sure that the name is unique within that cell.
Profile Name	DevNode	A unique profile name. It cannot begin with a period (.) and cannot contain any of the following special characters / \ * , ; = + ? < > & % ' " [] # \$ ^ { }.
Web Service Password	myWebSvcPwd	Password for the discovery web service API.
Web Service User	JohnDoe	User capable of modifying the managed environment through the discovery web service API.
WebSphere Binary Download Location	/opt/IBM/was	Fully qualified path to the compressed WebSphere software package on the target machine.
WebSphere Binary Files	WAS_V8.0_disk1.zip, WAS_V8.0_disk2.zip	Comma separated list of file names of the compressed WebSphere software packages.
WebSphere Extract Location	/opt/IBM/was	Fully qualified path where the compressed software will be extracted on the target machine. This location cannot be the same as Install Manager Extract Location.
WebSphere Install Location	/opt/IBM/WebSphere/AppServer	Fully qualified path where WebSphere will be installed.

Parameters for Provision WebSphere and Custom Node

The following tables describe the required and optional input parameters for this workflow. Most of these parameters are not initially visible in a deployment. For most parameters, if you do not specify a value for a parameter, a default value is assigned.

Input Parameters Defined in this Step: Gather Parameters for WebSphere Custom Node

Parameter Name	Default Value	Required	Description
Call Wrapper	see description	required	Command that will execute this step (or subsequent steps) as a specific user. Defaults are: UNIX targets: /opt/hp/dma/client/jython.sh running as root Windows targets: jython running as Administrator
Cell Name	no default	required	Unique cell name that does not contain any of the following special characters / \ * , ; = + ? < > & % ' " [] # \$ ^ { }. If you plan to federate into an existing cell later, make sure that this name is not the same as the existing cell name.
Dmgr Admin Password	no default	optional	Administrative user password for the Deployment Manager. When Enable Security is set to true, this parameter must contain a string that does not begin with a dash(-) or contain a space().
Dmgr Admin User	no default	optional	Deployment Manager administrative user. When Enable Security is set to true, this parameter must contain a string that does not begin with a dash(-), a period(.), or a space(). It cannot contain any of the following characters / \ * , ; = + ? < > & % ' " [] # \$ ^ { }.
Dmgr HostName	no default	optional	Host name or IP address of the machine where the Deployment Manager is running. Specify this parameter and the Dmgr Port parameter to federate the new custom node as it is created. If you do not specify a value for this parameter, the new custom node is not federated (you must federate it later). Required if Federate Later is set to false.
Dmgr Port	no default	optional	The SOAP port on which the Deployment Manager is listening. Specify this parameter and the Dmgr Host Name parameter to federate the new custom node as it is created. If you do not specify a value for this parameter, the new custom node is not federated (you must federate it later). Required if Federate Later is set to false.
Enable Security	no default	required	Enables administrative security on the Deployment Manager. Must be set to either true or false. If Enable Security is true, the Dmgr Admin User and Dmgr Admin Password parameters must have values.
Federate Later	no default	required	If false, the new custom node will be federated by the workflow during profile creation; you must specify Dmgr HostName and Dmgr Port to do this. If true, you must

Input Parameters Defined in this Step: Gather Parameters for WebSphere Custom Node, continued

Parameter Name	Default Value	Required	Description
			federate it later manually by using the addNode command.
Host Name	Server.name	required	Hostname or IP address of the target machine.
Install Manager Binary Download Location	/opt/IBM/iim	required	Fully qualified path to where the compressed Install Manager software package will be downloaded on the target machine. For example: /opt/IBM/iim
Install Manager Binary Files	no default	required	Name of the compressed Install Manager software package.
Install Manager Extract Location	no default	required	Fully qualified path where the compressed software will be extracted on the target machine. This location cannot be the same as WebSphere Extract Location.
Install Manager Install Location	no default	required	Fully qualified path where Install Manager will be installed. For example: /opt/IBM/InstallManager
License Acceptance	false	required	Acknowledges that the end user agrees to the IBM International Program License Agreement. This is set to false by default and must be set to true in order for the installation to continue.
Node Name	no default	required	Unique node name that cannot contain any of the following special characters / \ * , ; : = + ? [< > & % ' " [] # \$ ^ { }. If you plan to federate into an existing cell later, make sure that the name is unique within that cell.
Profile Name	no default	required	A unique profile name. It cannot begin with a period (.) and cannot contain any of the following special characters / \ * , ; : = + ? [< > & % ' " [] # \$ ^ { }.
Web Service Password	no default	required	Password for the discovery web service API.
Web Service User	no default	required	User capable of modifying the managed environment through the discovery web service API.
WebSphere Binary Download Location	/opt/IBM/WAS	required	Fully qualified path to the compressed WebSphere software package on the target machine.
WebSphere Binary Files	no default	required	Comma separated list of file names of the compressed WebSphere software packages.
WebSphere Extract Location	no default	required	Fully qualified path where the compressed software will be extracted on the target machine. This location cannot be the same as Install Manager Extract Location.

Input Parameters Defined in this Step: Gather Parameters for WebSphere Custom Node, continued

Parameter Name	Default Value	Required	Description
WebSphere Install Location	no default	required	Fully qualified path where WebSphere will be installed.
Windows Administrator Password	no default	required	The Windows Administrator password. Required for Windows.
Windows Administrator User	no default	required	This is the Windows Administrator user. Required for Windows.

Additional Input Parameters Defined in this Step: Gather Advanced Parameters for WebSphere Custom Node

Parameter Name	Default Value	Required	Description
Cleanup on Failure	True	optional	Indicates whether to remove downloaded and extracted files and to clean up the installation directory in the event of workflow failure. Valid values are True and False. The default is True, which will clean up on failure.
Cleanup on Success	True	optional	Indicates whether to remove downloaded and extracted files and to clean up the installation directory in the event of workflow success. Valid values are True and False. The default is True, which will clean up on success.
Keystore Password	no default	optional	Sets the password for all keystore files created during profile creation. This includes keystore files for both the default personal certificate and the root signing certificate.
Personal CertDN	no default	optional	Distinguished name of the personal certificate. For example: CN=dmlab-example.com,OU=WAS7LabCell,OU=WAS7LabDmgrManager,O=IBM,C=US The DN string cannot contain spaces. If you do not specify the DN, the WebSphere Application Server installer will create one.
Personal CertValidity Period	1	optional	Amount of time in years that the personal certificate is valid. Default is one year.
Ports File	no default	optional	Fully qualified path to a file that defines port settings for the new profile. This file must contain key=value pairs that specify a service name and a port number (for example: WC_adminhost=9060). This option should be used with the Validate Ports option.
Profile Response File	no default	optional	Fully qualified path where the response file that this workflow creates will be located. This file will then be used to drive the installation.
Response File	no default	optional	Fully qualified path where the response file that this workflow

Additional Input Parameters Defined in this Step: Gather Advanced Parameters for WebSphere Custom Node, continued

Parameter Name	Default Value	Required	Description
			creates will be located. This file will then be used to drive the installation and profile creation.
Signing CertDN	no default	optional	<p>Distinguished name of the signing certificate. For example: CN=dmalab-example.com, OU=Root Certificate, OU=WAS7TestLabCell, OU=WAS7LabNode1, O=IBM, C=US</p> <p>The DN string cannot contain spaces. If you do not specify the DN, the WebSphere Application Server installer will create one.</p>
Signing CertValidity Period	15	optional	Amount of time in years that the root certificate is valid. Default is 15 years.

Provision WebSphere Custom Node Profile From Existing Install

Use this workflow to create a custom profile on an existing WebSphere 8.0 or 8.5.x installation.

A custom profile initially contains an empty node with no servers. The workflow can add (federate) the server to the pertinent cell when the profile is created, or you can add it later yourself.

To use this workflow in your environment, see the following information:

Topic	Information Included
"Prerequisites for this Workflow"	List of prerequisites that must be satisfied before you can run this workflow
"How this Workflow Works"	Information about what the workflow does, including validation checks performed, steps executed, and a high-level process flow
"How to Run this Workflow"	Instructions for running this workflow in your environment
"Sample Scenario"	Examples of typical parameter values for this workflow
"Parameters for Provision WebSphere Custom Node Profile From Existing Install " on page 1135	List of input parameters for this workflow

Prerequisites for this Workflow

Be sure that the following prerequisites are satisfied before you run the WebSphere 8.0 or 8.5.x workflow:

1. This workflow requires unchallenged `sudo` access to a user (typically `root`) who can access all required files and directories.
2. Per the IBM WebSphere 8 documentation, the following system libraries are required before provisioning IBM WebSphere Application Server Network Deployment version 8.0 or 8.5.x on 64-bit and 32-bit Red Hat Linux targets:

Platform	Required Library
64-bit Red Hat Enterprise Linux version 5	compat-libstdc++-33-3.2.3-61 compat-db-4.2.52-5.1 gtk2-2.10.4-29.el5 gtk2-engines-2.8.0-3.el5 ksh-20080202-14 libXp-1.0.0-8 libXmu-1.0.2-5 libXtst-1.0.1-3.1 pam-0.99.6.2-3.26.el5 elfutils-0.125-3.el5 elfutils-libs-0.125-3.el5 libXft-2.1.10-1.1 libstdc++-4.1.2-48 <div> If the target server supports both 32-bit and 64-bit applications then both the 32-bit and 64-bit versions of the following libraries are required: </div> compat-libstdc++-33-3.2.3-61 compat-db-4.2.52-5.1 gtk2-2.18.9-4 gtk2-engines-2.18.4-5 libstdc++-4.1.2-48 libXft-2.1.10-1.1 libXp-1.0.0-8 libXmu-1.0.2-5 libXtst-1.0.1-3.1 pam-0.99.6.2-3.26.el5
64-bit Red Hat Enterprise Linux version 6	compat-libstdc++-33-3.2.3-69 compat-db-4.6.21-15 ksh-20100621-2 gtk2-2.18.9-4 gtk2-engines-2.18.4-5 libXp-1.0.0-15.1 libXmu-1.0.5-1 libXtst-1.0.99.2-3

Platform	Required Library
	<p>pam-1.1.1-4 elfutils-0.148-1 elfutils-libs-0.148-1 libXft-2.1.13-4.1 libstdc++-4.4.4-13</p> <p>If the target server supports both 32-bit and 64-bit applications then both the 32-bit and 64-bit versions of the following libraries are required:</p> <p>compat-libstdc++-33-3.2.3-69 compat-db-4.6.21-15 libstdc++-4.4.4-13 libXp-1.0.0-15.1 libXmu-1.0.5-1 libXtst-1.0.99.2-3 pam-1.1.1-4 libXft-2.1.13-4.1 gtk2-2.18.9-4 gtk2-engines-2.18.4-5</p>

Make sure that these libraries exist on each target server before running this workflow. If newer versions of these libraries are available, you can install the newer versions.

3. This workflow will install WebSphere Application Server as root because of the following IBM documented limitations:
 - Creation of a Linux service for WebSphere Application Server
 - Native registration with the operating system
 - Port conflicts that may occur with other installations of WebSphere Application Server that are not registered with the operating system

If there is a need to run as a non-root user after installation, you can run a recursive `chown` under the installation root and set owner permissions accordingly.

For more information about prerequisites for WebSphere 8, refer to the [WebSphere 8 Product Documentation](#).

How this Workflow Works

This topic contains the following information about the "[Provision WebSphere Custom Node Profile From Existing Install](#)" workflow:

Overview

This workflow creates a Custom Node profile on an existing WebSphere 8.0 or 8.5.x installation.

See the following topics for detailed information:

[Validation Checks Performed](#)

[Steps in this Workflow](#)

[Process Flow](#)

Validation Checks Performed

Most of the validation centers on special characters and spaces in the parameters. There are also validation checks that happen at the operating system level, including file system space checks and RPM checks (on Red Hat Linux platforms only).

The workflow first performs the following parameter checks:

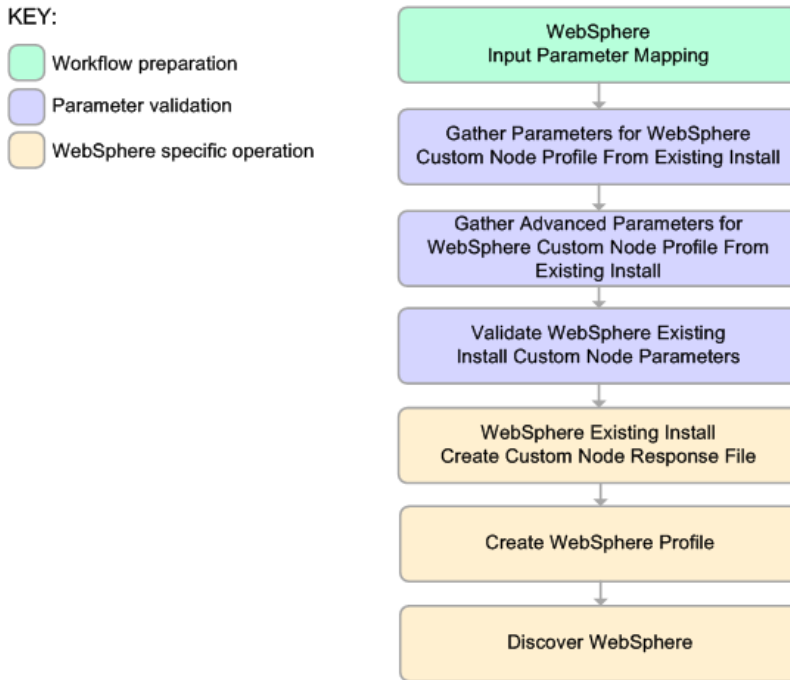
1. Required parameters have values specified.
2. WebSphere specific names do not contain the following characters: `/ \ * , ; = + ? | < > & % ' " [] # $ ^ { }`
3. Parameters do not contain illegal characters for the parameter type.
4. Flag parameters are set to true or false.
5. Integer parameters are set to appropriate integer values.
6. Mutually dependent parameters are specified appropriately as a set.
7. Parameters are set to one of the values if the parameter has a list of valid values.
8. License Acceptance is true (for workflows that input the License Acceptance parameter).
9. All specified file names are legal file names.
10. All specified locations are legal path names. If they do not exist they will be created.

Note: For more information about valid parameter values, see ["Parameters for Provision WebSphere Custom Node Profile From Existing Install "](#).

The workflow then checks to make sure that all required libraries are present on the target machine (see ["Prerequisites for this Workflow"](#)).

Steps Executed

The Provision WebSphere Stand-Alone Profile From Existing Install workflow includes the following steps. Each step must complete successfully before the next step can start. If a step fails, the workflow reports a failure, and all subsequent steps are skipped.



Process Flow

This workflow performs the following tasks:

1. Creates the call wrapper and determines the target server platform type.
2. Gathers and validates the parameters needed to create a Custom Node profile (see "[Validation Checks Performed](#)" on the previous page).
3. Creates a new response file for the purpose of creating a Custom Node profile on top of the existing WebSphere 8.0 or 8.5.x installation.
4. Creates a Custom Node profile on top of the WebSphere 8.0 or 8.5.x installation.
5. Federates into the Deployment Manager.
6. Discovers any WebSphere 8.0 or 8.5.x cells, clusters, and managed servers associated with the Profile Root that you specify. If these items are found, they are added to the DMA environment.

How to Run this Workflow

The following instructions show you how to customize and run the ["Provision WebSphere Custom Node Profile From Existing Install"](#) workflow in your environment.

The workflow provides default values for some parameters. These default values are usually sufficient for a "typical" installation. You can override the defaults by specifying parameter values in the deployment. You can also expose additional parameters in the workflow, if necessary, to accomplish more advanced scenarios. Any parameters not explicitly specified in the deployment will have the default values listed in ["Parameters for Provision WebSphere Custom Node Profile From Existing Install"](#).

Note: Before following this procedure, review the ["Prerequisites for this Workflow"](#), and ensure that all requirements are satisfied.

To use the Provision WebSphere Stand-Alone Profile From Existing Install workflow:

1. Create a deployable copy of the workflow
2. Determine the values that you will specify for the following parameters:

Parameters Defined in this Step: Gather Parameters for WebSphere Existing Install Stand Alone

Parameter Name	Default Value	Required	Description
Cell Name	no default	required	Unique cell name that does not contain any of the following special characters <code>/ \ * , : ; = + ? < > & % ' " [] # \$ ^ { }</code> . If you plan to federate into an existing cell later, make sure that this name is not the same as the existing cell name.
Dmgr Admin Password	no default	optional	Administrative user password for the Deployment Manager. When Enable Security is set to true, this parameter must contain a string that does not begin with a dash(-) or contain a space().
Dmgr Admin User	no default	optional	Deployment Manager administrative user. When Enable Security is set to true, this parameter must contain a string that does not begin with a dash(-), a period(.), or a space(). It cannot contain any of the following characters <code>/ \ * , : ; = + ? < > & % ' " [] # \$ ^ { }</code> .
Dmgr HostName	no default	optional	Host name or IP address of the machine where the Deployment Manager is running. Specify this parameter and the Dmgr Port parameter to federate the new custom node as it is created. If you do not specify a value for this parameter, the new custom node is not federated (you must federate it later). Required if Federate Later is set to false.

Parameters Defined in this Step: Gather Parameters for WebSphere Existing Install Stand Alone , continued

Parameter Name	Default Value	Required	Description
Dmgr Port	no default	optional	The SOAP port on which the Deployment Manager is listening. Specify this parameter and the Dmgr Host Name parameter to federate the new custom node as it is created. If you do not specify a value for this parameter, the new custom node is not federated (you must federate it later). Required if Federate Later is set to false.
Enable Security	no default	required	Enables administrative security on the Deployment Manager. Must be set to either true or false. If Enable Security is true, the Dmgr Admin User and Dmgr Admin Password parameters must have values.
Node Name	no default	required	Unique node name that cannot contain any of the following special characters / \ * , ; = + ? < > & % ' " [] # \$ ^ { }. If you plan to federate into an existing cell later, make sure that the name is unique within that cell.
Profile Name	no default	required	A unique profile name. It cannot begin with a period (.) and cannot contain any of the following special characters / \ * , ; = + ? < > & % ' " [] # \$ ^ { }.
Web Service Password	no default	required	Password for the discovery web service API.
Web Service User	no default	required	User capable of modifying the managed environment through the discovery web service API.
WebSphere Install Location	no default	required	Fully qualified path where WebSphere will be installed.
Windows Administrator Password	no default	required	The Windows Administrator password. Required for Windows.
Windows Administrator User	no default	required	This is the Windows Administrator user. Required for Windows.

Note: This is the minimum set of parameters required to run this workflow. You may need to expose additional parameters depending on your provisioning objectives.

See ["Parameters for Provision WebSphere Custom Node Profile From Existing Install "](#) for detailed descriptions of all input parameters for this workflow, including default values.

Tip: To avoid having to re-enter passwords whenever they change, you can create a policy to provide them to the workflow.

3. In the workflow editor, expose any additional parameters that you need. You will specify values for those parameters when you create the deployment.
4. Save the changes to the workflow (click **Save** in the lower right corner).
5. Create a new deployment.
6. On the Parameters tab, specify values for the required parameters listed in step 2 and any additional parameters that you have exposed. You do not need to specify values for those parameters whose default values are appropriate for your environment.
7. On the Targets tab, specify one or more targets for this deployment.
8. Save the deployment (click **Save** in the lower right corner).
9. Run the workflow using this deployment.

To verify the results:

The workflow will complete and report SUCCESS on the Console if it has run successfully. If an error occurs during workflow execution, the error is logged, and the workflow terminates in the FAILURE state.

Be sure to also perform the following steps:

1. After the workflow has completed, run the following command to check the version of WebSphere Application Server that was installed:

```
WAS_ROOT/bin/versionInfo.sh
```

Here, *WAS_ROOT* is the directory where WebSphere 8.0 or 8.5.x is installed. This is the path that you specified in the WebSphere Install Location parameter.

2. Validate that the profile has been created and is running by doing the following:
 - a. View the *WAS_ROOT*/profiles/*PROFILE_NAME*/logs/AboutThisProfile.txt file. This file is created after the creation of the profile and contains specific information about the profile.

Here, *PROFILE_NAME* is the name of the profile that you just created. This is the name that you specified in the Profile Name parameter.

- b. Change to the *WAS_ROOT*/profiles/*PROFILE_NAME*/logs/*CELL_NAME* directory, and tail the SystemOut.log file. Look for the following line:

```
Server CELL_NAME open for e-business
```

Here, *CELL_NAME* is the name of the WebSphere 8.0 or 8.5.x cell to which this profile pertains. This is the name that you specified in the Cell Name parameter.

Sample Scenario

This topic shows you typical parameter values used for the ["Provision WebSphere Custom Node Profile From Existing Install"](#) workflow.

Tip: To avoid having to re-enter passwords whenever they change, you can create a policy to provide them to the workflow.

Custom Node Profiles on Existing Install – Parameter Value Examples

Parameter Name	Example Value	Description
Cell Name	Dev NodeCell	Unique cell name that does not contain any of the following special characters <code>/ \ * , ; = + ? < > & % ' " [] # \$ ^ { }</code> . If you plan to federate into an existing cell later, make sure that this name is not the same as the existing cell name.
Dmgr Admin Password	wasPassWord	Administrative user password for the Deployment Manager. When Enable Security is set to true, this parameter must contain a string that does not begin with a dash(-) or contain a space().
Dmgr Admin User	wasadmin	Deployment Manager administrative user. When Enable Security is set to true, this parameter must contain a string that does not begin with a dash(-), a period(.), or a space(). It cannot contain any of the following characters <code>/ \ * , ; = + ? < > & % ' " [] # \$ ^ { }</code> .
Dmgr HostName	testserver.mycompany.com	Host name or IP address of the machine where the Deployment Manager is running. Specify this parameter and the Dmgr Port parameter to federate the new custom node as it is created. If you do not specify a value for this parameter, the new custom node is not federated (you must federate it later). Required if Federate Later is set to false.
Dmgr Port	8879	The SOAP port on which the Deployment Manager is listening. Specify this parameter and the Dmgr Host Name parameter to federate the new custom node as it is created. If you do not specify a value for this parameter, the new custom node is not federated (you must federate it later). Required if Federate Later is set to false.
Enable Security	true	Enables administrative security on the Deployment Manager. Must be set to either true or false. If Enable Security is true, the Dmgr Admin User and Dmgr Admin Password parameters must have values.
Node Name	DevNode1	Unique node name that cannot contain any of the following special characters <code>/ \ * , ; = + ? < > & % ' " [] # \$ ^ { }</code> . If you plan to federate into an existing cell later, make sure that the name is unique within that cell.
Profile	DevNode1	A unique profile name. It cannot begin with a period (.)

Custom Node Profiles on Existing Install – Parameter Value Examples , continued

Parameter Name	Example Value	Description
Name		and cannot contain any of the following special characters <code>/ \ * , : ; = + ? < > & % ' " [] # \$ ^ { }</code> .
Web Service Password	myWebSvcPwd	Password for the discovery web service API.
Web Service User	JohnDoe	User capable of modifying the managed environment through the discovery web service API.
WebSphere Install Location	/opt/IBM/WebSphere/AppServer	Fully qualified path where WebSphere will be installed.

Parameters for Provision WebSphere Custom Node Profile From Existing Install

The following tables describe the required and optional input parameters for this workflow. Most of these parameters are not initially visible in a deployment. For most parameters, if you do not specify a value for a parameter, a default value is assigned.

Input Parameters Defined in this Step: Gather Parameters for WebSphere Existing Install Stand Alone

Parameter Name	Default Value	Required	Description
Call Wrapper	see description	required	Command that will execute this step (or subsequent steps) as a specific user. Defaults are: UNIX targets: /opt/hp/dma/client/jython.sh running as root Windows targets: jython running as Administrator
Cell Name	no default	required	Unique cell name that does not contain any of the following special characters <code>/ \ * , ; = + ? < > & % ' " [] # \$ ^ { }</code> . If you plan to federate into an existing cell later, make sure that this name is not the same as the existing cell name.
Dmgr Admin Password	no default	optional	Administrative user password for the Deployment Manager. When Enable Security is set to true, this parameter must contain a string that does not begin with a dash(-) or contain a space().
Dmgr Admin User	no default	optional	Deployment Manager administrative user. When Enable Security is set to true, this parameter must contain a string that does not begin with a dash(-), a period(.), or a space(). It cannot contain any of the following characters <code>/ \ * , ; = + ? < > & % ' " [] # \$ ^ { }</code> .
Dmgr HostName	no default	optional	Host name or IP address of the machine where the Deployment Manager is running. Specify this parameter and the Dmgr Port parameter to federate the new custom node as it is created. If you do not specify a value for this parameter, the new custom node is not federated (you must federate it later). Required if Federate Later is set to false.
Dmgr Port	no default	optional	The SOAP port on which the Deployment Manager is listening. Specify this parameter and the Dmgr Host Name parameter to federate the new custom node as it is created. If you do not specify a value for this parameter, the new custom node is not federated (you must federate it later). Required if Federate Later is set to false.
Enable Security	no default	required	Enables administrative security on the Deployment Manager. Must be set to either true or false. If Enable Security is true, the Dmgr Admin User and Dmgr Admin Password parameters must have values.

Input Parameters Defined in this Step: Gather Parameters for WebSphere Existing Install Stand Alone , continued

Parameter Name	Default Value	Required	Description
Host Name	Server.name	required	Hostname or IP address of the target machine.
Node Name	no default	required	Unique node name that cannot contain any of the following special characters <code>/ \ * , ; = + ? < > & % ' " [] # \$ ^ { }</code> . If you plan to federate into an existing cell later, make sure that the name is unique within that cell.
Profile Name	no default	required	A unique profile name. It cannot begin with a period (.) and cannot contain any of the following special characters <code>/ \ * , ; = + ? < > & % ' " [] # \$ ^ { }</code> .
Web Service Password	no default	required	Password for the discovery web service API.
Web Service User	no default	required	User capable of modifying the managed environment through the discovery web service API.
WebSphere Install Location	no default	required	Fully qualified path where WebSphere will be installed.
Windows Administrator Password	no default	required	The Windows Administrator password. Required for Windows.
Windows Administrator User	no default	required	This is the Windows Administrator user. Required for Windows.

Additional Input Parameters Defined in this Step: Gather Advanced Parameters for WebSphere Existing Install Stand Alone

Parameter Name	Default Value	Required	Description
Keystore Password	no default	optional	Sets the password for all keystore files created during profile creation. This includes keystore files for both the default personal certificate and the root signing certificate.
Personal CertDN	no default	optional	Distinguished name of the personal certificate. For example: CN=dmlab-example.com,OU=WAS7LabCell,OU=WAS7LabDmgrManager,O=IBM,C=US The DN string cannot contain spaces. If you do not specify the DN, the WebSphere Application Server installer will create one.
Personal CertValidity Period	1	optional	Amount of time in years that the personal certificate is valid. Default is one year.
Ports File	no default	optional	Fully qualified path to a file that defines port settings for the new profile. This file must contain key=value pairs that specify a service name and a port number (for example: WC_

Additional Input Parameters Defined in this Step: Gather Advanced Parameters for WebSphere Existing Install Stand Alone, continued

Parameter Name	Default Value	Required	Description
			adminhost=9060). This option should be used with the Validate Ports option.
Profile Response File	no default	optional	Fully qualified path where the response file that this workflow creates will be located. This file will then be used to drive the installation.
Response File	no default	optional	Fully qualified path where the response file that this workflow creates will be located. This file will then be used to drive the installation and profile creation.
Signing CertDN	no default	optional	<p>Distinguished name of the signing certificate. For example: CN=dmlab-example.com, OU=Root Certificate, OU=WAS7TestLabCell, OU=WAS7LabNode1, O=IBM, C=US</p> <p>The DN string cannot contain spaces. If you do not specify the DN, the WebSphere Application Server installer will create one.</p>
Signing CertValidity Period	15	optional	Amount of time in years that the root certificate is valid. Default is 15 years.

Provision WebSphere and Deployment Manager

Use this workflow to install a new instance of the IBM WebSphere Application Server Network Deployment version 8.0 or 8.5.x and Installation Manager, and then create a deployment manager profile.

A deployment manager is the administration point for a cell that contains multiple application servers. This type of profile is appropriate for distributed application server environments.

To use this workflow in your environment, see the following information:

Topic	Information Included
"Prerequisites for this Workflow"	List of prerequisites that must be satisfied before you can run this workflow
"How this Workflow Works"	Information about what the workflow does, including validation checks performed, steps executed, and a high-level process flow
"How to Run this Workflow"	Instructions for running this workflow in your environment
"Sample Scenario"	Examples of typical parameter values for this workflow
Parameters	List of input parameters for this workflow

Note: The documentation for this workflow contains steps that are referred to by their base names. The names in the DMA user interface may have a version appended, for example, v2.

Prerequisites for this Workflow

Be sure that the following prerequisites are satisfied before you run the Provision WebSphere and Deployment Manager workflow:

1. This workflow requires unchallenged `sudo` access to a user (typically `root`) who can access all required files and directories.
2. Per the IBM WebSphere 8 documentation, the following system libraries are required before provisioning IBM WebSphere Application Server Network Deployment version 8.0 or 8.5.x on 64-bit and 32-bit Red Hat Linux targets:

Platform	Required Library
64-bit Red Hat Enterprise Linux version 5	<p> compat-libstdc++-33-3.2.3-61 compat-db-4.2.52-5.1 gtk2-2.10.4-29.el5 gtk2-engines-2.8.0-3.el5 ksh-20080202-14 libXp-1.0.0-8 libXmu-1.0.2-5 libXtst-1.0.1-3.1 pam-0.99.6.2-3.26.el5 elfutils-0.125-3.el5 elfutils-libs-0.125-3.el5 libXft-2.1.10-1.1 libstdc++-4.1.2-48 </p> <p> If the target server supports both 32-bit and 64-bit applications then both the 32-bit and 64-bit versions of the following libraries are required: </p> <p> compat-libstdc++-33-3.2.3-61 compat-db-4.2.52-5.1 gtk2-2.18.9-4 gtk2-engines-2.18.4-5 libstdc++-4.1.2-48 libXft-2.1.10-1.1 libXp-1.0.0-8 libXmu-1.0.2-5 libXtst-1.0.1-3.1 pam-0.99.6.2-3.26.el5 </p>
64-bit Red Hat Enterprise Linux version 6	<p> compat-libstdc++-33-3.2.3-69 compat-db-4.6.21-15 ksh-20100621-2 gtk2-2.18.9-4 gtk2-engines-2.18.4-5 libXp-1.0.0-15.1 libXmu-1.0.5-1 libXtst-1.0.99.2-3 </p>

Platform	Required Library
	<p>pam-1.1.1-4 elfutils-0.148-1 elfutils-libs-0.148-1 libXft-2.1.13-4.1 libstdc++-4.4.4-13</p> <p>If the target server supports both 32-bit and 64-bit applications then both the 32-bit and 64-bit versions of the following libraries are required:</p> <p>compat-libstdc++-33-3.2.3-69 compat-db-4.6.21-15 libstdc++-4.4.4-13 libXp-1.0.0-15.1 libXmu-1.0.5-1 libXtst-1.0.99.2-3 pam-1.1.1-4 libXft-2.1.13-4.1 gtk2-2.18.9-4 gtk2-engines-2.18.4-5</p>

Make sure that these libraries exist on each target server before running this workflow. If newer versions of these libraries are available, you can install the newer versions.

3. This workflow will install WebSphere Application Server as root because of the following IBM documented limitations:
 - Creation of a Linux service for WebSphere Application Server
 - Native registration with the operating system
 - Port conflicts that may occur with other installations of WebSphere Application Server that are not registered with the operating system

If there is a need to run as a non-root user after installation, you can run a recursive `chown` under the installation root and set owner permissions accordingly.

For more information about prerequisites for WebSphere 8, refer to the [WebSphere 8 Product Documentation](#).

How this Workflow Works

This topic contains the following information about the "[Provision WebSphere and Deployment Manager](#)" workflow:

Overview

This workflow does the following three things in the order shown:

1. Installs the IBM Install Manager
2. Installs IBM WebSphere Application Server Network Deployment version 8.0 or 8.5.x
3. Creates a Deployment Manager profile

The workflow checks to see if the WebSphere 8.0 or 8.5.x binary archive files exist on the target machine. If they do not, the files are downloaded from the software repository.

See the following topics for detailed information:

[Validation Checks Performed](#)

[Steps in this Workflow](#)

[Process Flow](#)

Note: This workflow has been updated to account for the significant changes in the way that WebSphere 8 are installed.

Validation Checks Performed

Most of the validation centers on special characters and spaces in the parameters. There are also validation checks that happen at the operating system level, including file system space checks and RPM checks (on Red Hat Linux platforms only).

The workflow first performs the following parameter checks:

1. Required parameters have values specified.
2. WebSphere specific names do not contain the following characters: `/ \ * , ; = + ? | < > & % ' " [] # $ ^ { }`
3. Parameters do not contain illegal characters for the parameter type.
4. Flag parameters are set to true or false.
5. Integer parameters are set to appropriate integer values.
6. Mutually dependent parameters are specified appropriately as a set.
7. Parameters are set to one of the values if the parameter has a list of valid values.
8. License Acceptance is true (for workflows that input the License Acceptance parameter).
9. All specified file names are legal file names.
10. All specified locations are legal path names. If they do not exist they will be created.

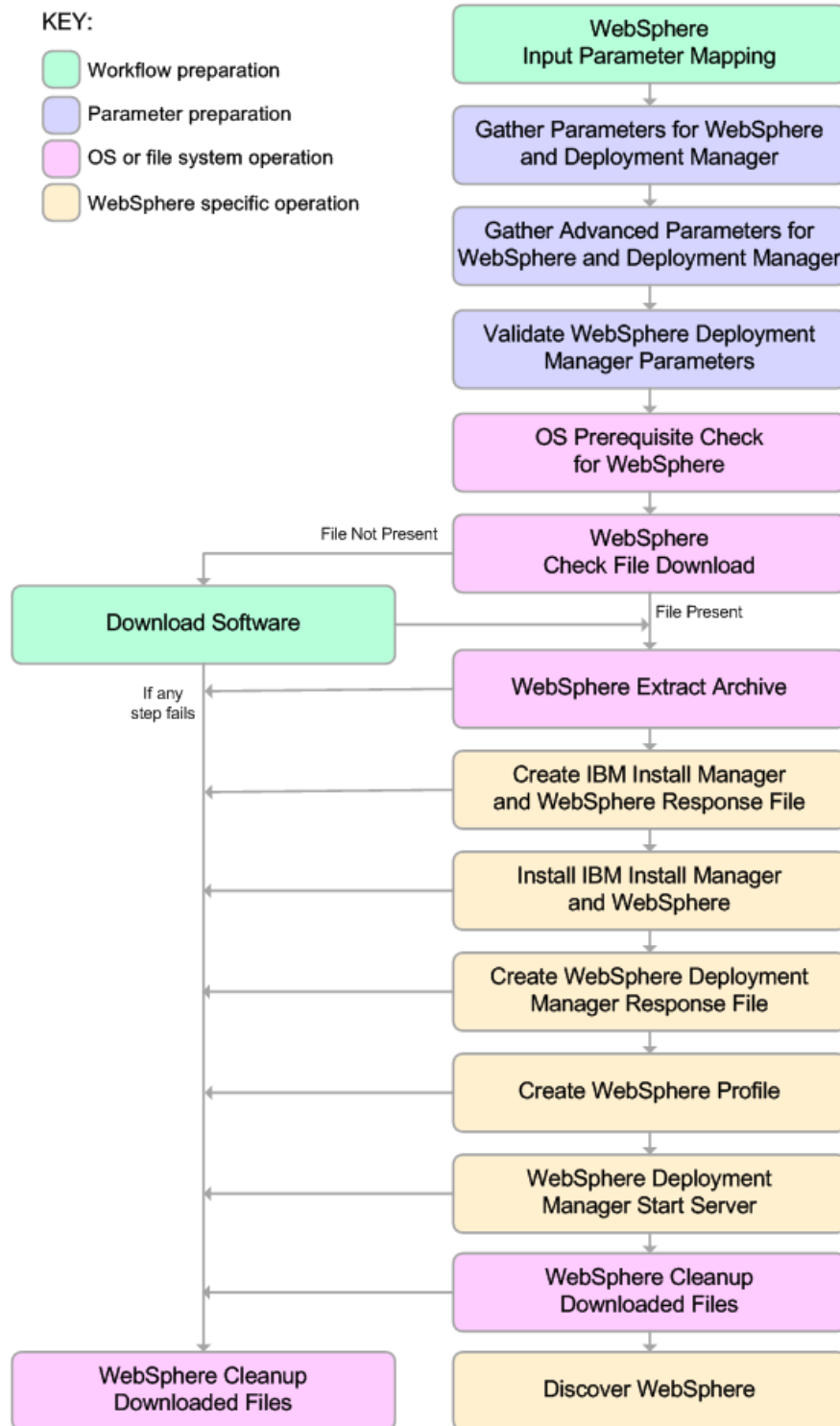
Note: For more information about valid parameter values, see ["Parameters for Provision WebSphere and Deployment Manager"](#).

The workflow then performs the following operating system checks on the target machine:

1. All required libraries are present (see ["Prerequisites for this Workflow"](#)).
2. Sufficient disk space is available to install WebSphere 8.0 or 8.5.x.
3. Sufficient disk space is available to extract the binary files from the compressed archive.

Steps Executed

The Provision WebSphere and Deployment Manager workflow includes the following steps. Each step must complete successfully before the next step can start. If a step fails, the workflow reports a failure, and all subsequent steps are skipped.



Process Flow

This workflow performs the following tasks:

1. Creates the call wrapper and determines the target server platform type.
2. Gathers and validates the parameters needed to install WebSphere 8.0 or 8.5.x and create a Deployment Manager profile (see ["Validation Checks Performed " on page 1142](#)).
3. Checks the following:
 - a. Documented library requirements for WebSphere 8 (see the ["Prerequisites for this Workflow"](#)).
 - b. File system space requirements where WebSphere 8.0 or 8.5.x will be installed.
 - c. Temporary space requirements where the compressed software will be extracted before it is installed.
4. Determines whether the WebSphere 8.0 or 8.5.x binary archive is present on the target machine. If the archive is not present, the workflow downloads it from the software repository.
5. Extracts the WebSphere 8.0 or 8.5.x binary archive to the specified directory.
6. Creates a response file for the purpose of installing a new instance of WebSphere 8.0 or 8.5.x.
7. Installs the IBM Installation Manager and a new WebSphere 8.0 or 8.5.x instance on the target server.
8. Creates a new response file for the purpose of creating a Deployment Manager profile on top of the WebSphere 8.0 or 8.5.x installation.
9. Creates a Deployment Manager profile on top of the WebSphere 8.0 or 8.5.x installation.
10. Starts the new Deployment Manager WebSphere 8.0 or 8.5.x application server.
11. Cleans up any files that were downloaded—for either workflow success or failure.

Note: The parameters Cleanup on Success and Cleanup on Failure are defaulted to True. If they are set to False, the downloaded files are not cleaned up.

12. Discovers any WebSphere 8.0 or 8.5.x cells, clusters, and managed servers associated with the Profile Root that you specify. If these items are found, they are added to the DMA environment.

How to Run this Workflow

The following instructions show you how to customize and run the "[Provision WebSphere and Deployment Manager](#)" workflow in your environment.

The workflow provides default values for some parameters. These default values are usually sufficient for a "typical" installation. You can override the defaults by specifying parameter values in the deployment. You can also expose additional parameters in the workflow, if necessary, to accomplish more advanced scenarios. Any parameters not explicitly specified in the deployment will have the default values listed in "[Parameters for Provision WebSphere and Deployment Manager](#)".

Note: Before following this procedure, review the "[Prerequisites for this Workflow](#)", and ensure that all requirements are satisfied.

To customize and run the Provision WebSphere and Deployment Manager workflow:

1. Create a deployable copy of the workflow.
2. Determine the values that you will specify for the following parameters:

Parameters Defined in this Step: Gather Parameters for WebSphere and Deployment Manager

Parameter Name	Default Value	Required	Description
Admin Password	no default	optional	When Enable Security is set to true, this parameter must contain a string that does not begin with a dash(-) or contain a space().
Admin User	no default	optional	When Enable Security is set to true, this parameter must contain a string that does not begin with a dash(-), a period(.), or a space(). It cannot contain any of the following characters / \ * , ; = + ? < > & % ' " [] # \$ ^ { }.
Cell Name	no default	required	Unique cell name that does not contain any of the following special characters / \ * , ; = + ? < > & % ' " [] # \$ ^ { }. If you plan to federate into an existing cell later, make sure that this name is not the same as the existing cell name.
Enable Security	no default	required	Enables administrative security. Must be set to either true or false. If Enable Security is true, the Admin User and Admin Password parameters must have values.
Install Manager Binary Download Location	/opt/IBM/iim	required	Fully qualified path to where the compressed Install Manager software package will be downloaded on the target machine. For example: /opt/IBM/iim

Parameters Defined in this Step: Gather Parameters for WebSphere and Deployment Manager, continued

Parameter Name	Default Value	Required	Description
Install Manager Binary Files	no default	required	Name of the compressed Install Manager software package.
Install Manager Extract Location	no default	required	Fully qualified path where the compressed software will be extracted on the target machine. This location cannot be the same as WebSphere Extract Location.
Install Manager Install Location	no default	required	Fully qualified path where Install Manager will be installed. For example: /opt/IBM/InstallManager
License Acceptance	false	required	Acknowledges that the end user agrees to the IBM International Program License Agreement. This is set to false by default and must be set to true in order for the installation to continue.
Node Name	no default	required	Unique node name that cannot contain any of the following special characters / \ * , ; = + ? < > & % ' " [] # \$ ^ { }. If you plan to federate into an existing cell later, make sure that the name is unique within that cell.
Profile Name	no default	required	A unique profile name. It cannot begin with a period (.) and cannot contain any of the following special characters / \ * , ; = + ? < > & % ' " [] # \$ ^ { }.
Web Service Password	no default	required	Password for the discovery web service API.
Web Service User	no default	required	User capable of modifying the managed environment through the discovery web service API.
WebSphere Binary Download Location	/opt/IBM/WAS	required	Fully qualified path to the compressed WebSphere software package on the target machine.
WebSphere Binary Files	no default	required	Comma separated list of file names of the compressed WebSphere software packages.
WebSphere Extract Location	no default	required	Fully qualified path where the compressed software will be extracted on the target machine. This location cannot be the same as Install Manager Extract Location.
WebSphere Install Location	no default	required	Fully qualified path where WebSphere will be installed.

Parameters Defined in this Step: Gather Parameters for WebSphere and Deployment Manager, continued

Parameter Name	Default Value	Required	Description
Windows Administrator Password	no default	required	The Windows Administrator password. Required for Windows.
Windows Administrator User	no default	required	This is the Windows Administrator user. Required for Windows.

Note: This is the minimum set of parameters required to run this workflow. You may need to expose additional parameters depending on your provisioning objectives.

See ["Parameters for Provision WebSphere and Deployment Manager"](#) for detailed descriptions of all input parameters for this workflow, including default values.

3. In the workflow editor, expose any additional parameters that you need. You will specify values for those parameters when you create the deployment.
4. Save the changes to the workflow (click **Save** in the lower right corner).
5. Create a new deployment.
6. On the Parameters tab, specify values for the required parameters listed in step 2 and any additional parameters that you have exposed. You do not need to specify values for those parameters whose default values are appropriate for your environment.
7. On the Targets tab, specify one or more targets for this deployment.
8. Save the deployment (click **Save** in the lower right corner).
9. Run the workflow using this deployment.

To verify the results:

The workflow will complete and report SUCCESS on the Console if it has run successfully. If an error occurs during workflow execution, the error is logged, and the workflow terminates in the FAILURE state.

Be sure to also perform the following steps:

1. After the workflow has completed, run the following command to check the version of WebSphere Application Server that was installed:

```
WAS_ROOT/bin/versionInfo.sh
```

Here, *WAS_ROOT* is the directory where WebSphere 8.0 or 8.5.x is installed. This is the path that you specified in the WebSphere Install Location parameter.

2. Validate that the profile has been created and is running by doing the following:
 - a. View the *WAS_ROOT*/profiles/*PROFILE_NAME*/logs/AboutThisProfile.txt file. This file is created after the creation of the profile and contains specific information about the profile.

Here, *PROFILE_NAME* is the name of the profile that you just created. This is the name that you specified in the Profile Name parameter.

- b. Change to the *WAS_ROOT*/profiles/*PROFILE_NAME*/logs/*CELL_NAME* directory, and tail the SystemOut.log file. Look for the following line:

```
Server CELL_NAME open for e-business
```

Here, *CELL_NAME* is the name of the WebSphere 8.0 or 8.5.x cell to which this profile pertains. This is the name that you specified in the Cell Name parameter.

Sample Scenario

This topic shows you typical parameter values used for the "[Provision WebSphere and Deployment Manager](#)" workflow.

Tip: To avoid having to re-enter passwords whenever they change, you can create a policy to provide them to the workflow.

New Install with Deployment Manager – Parameter Value Examples

Parameter Name	Example Value	Description
Admin Password	wasPassWord	When Enable Security is set to true, this parameter must contain a string that does not begin with a dash(-) or contain a space().
Admin User	wasadmin	When Enable Security is set to true, this parameter must contain a string that does not begin with a dash(-), a period (.), or a space(). It cannot contain any of the following characters / \ * , ; ; = + ? < > & % ' " [] # \$ ^ { }.
Cell Name	DevCell	Unique cell name that does not contain any of the following special characters / \ * , ; ; = + ? < > & % ' " [] # \$ ^ { }. If you plan to federate into an existing cell later, make sure that this name is not the same as the existing cell name.
Enable Security	true	Enables administrative security. Must be set to either true or false. If Enable Security is true, the Admin User and Admin Password parameters must have values.
Host Name	/opt/IBM/iim	Fully qualified path to where the compressed Install Manager software package will be downloaded on the target machine. For example: /opt/IBM/iim
Install Manager Binary Download Location	IBM_Install_Manager_Linux.zip	Name of the compressed Install Manager software package.
Install Manager Binary Files	/opt/IBM/iim	Fully qualified path where the compressed software will be extracted on the target machine. This location cannot be the same as Install Manager Extract Location.
Install Manager Extract Location	/opt/IBM/installManager	Fully qualified path where Install Manager will be installed. For example: /opt/IBM/InstallManager
Install Manager Install Location	true	Acknowledges that the end user agrees to the IBM International Program License Agreement. This is set to false by default and must be set to true in order for the installation to continue.
License Acceptance	DevManager	Unique node name that cannot contain any of the following special characters / \ * , ; ; = + ? < > & % ' " [] # \$ ^ { }. If you plan to federate into an existing cell later, make sure

New Install with Deployment Manager – Parameter Value Examples, continued

Parameter Name	Example Value	Description
		that the name is unique within that cell.
Node Name	DevDmgr	A unique profile name. It cannot begin with a period (.) and cannot contain any of the following special characters / \ * , ; = + ? < > & % ' " [] # \$ ^ { }.
Profile Name	myWebSvcPwd	Password for the discovery web service API.
Web Service Password	JohnDoe	User capable of modifying the managed environment through the discovery web service API.
Web Service User	/opt/IBM/was	Fully qualified path to the compressed WebSphere software package on the target machine.
WebSphere Binary Download Location	WAS_V8.0_disk1.zip, WAS_V8.0_disk2.zip, WAS_V8.0_disk3.zip, WAS_V8.0_disk4.zip	Comma separated list of file names of the compressed WebSphere software packages.
WebSphere Binary Files	/opt/IBM/was	Fully qualified path where the compressed software will be extracted on the target machine. This location cannot be the same as Install Manager Extract Location.
WebSphere Extract Location	/opt/IBM/ WebSphere/AppServer	Fully qualified path where WebSphere will be installed.

Parameters for Provision WebSphere and Deployment Manager

The following tables describe the required and optional input parameters for this workflow. Most of these parameters are not initially visible in a deployment. For most parameters, if you do not specify a value for a parameter, a default value is assigned

Input Parameters Defined in this Step: Gather Parameters for WebSphere and Deployment Manager

Parameter Name	Default Value	Required	Description
Admin Password	no default	optional	When Enable Security is set to true, this parameter must contain a string that does not begin with a dash (-) or contain a space ().
Admin User	no default	optional	When Enable Security is set to true, this parameter must contain a string that does not begin with a dash(-), a period(.), or a space(). It cannot contain any of the following characters / \ * , ; ; = + ? < > & % ' " [] # \$ ^ { }.
Call Wrapper	see description	required	Command that will execute this step (or subsequent steps) as a specific user. Defaults are: UNIX targets: /opt/hp/dma/client/jython.sh running as root Windows targets: jython running as Administrator
Cell Name	no default	optional	Unique cell name that does not contain any of the following special characters / \ * , ; ; = + ? < > & % ' " [] # \$ ^ { }. If you plan to federate into an existing cell later, make sure that this name is not the same as the existing cell name.
Enable Security	no default	optional	Enables administrative security. Must be set to either true or false. If Enable Security is true, the Admin User and Admin Password parameters must have values.
Host Name	Server.name	required	Hostname or IP address of the target machine.
Install Manager Binary Download Location	/opt/IBM/iim	required	Fully qualified path to where the compressed Install Manager software package will be downloaded on the target machine. For example: /opt/IBM/iim
Install Manager Binary Files	no default	required	Name of the compressed Install Manager software package.
Install Manager Extract Location	no default	required	Fully qualified path where the compressed software will be extracted on the target machine. This location cannot be the same as WebSphere Extract Location.
Install Manager Install Location	no default	required	Fully qualified path where Install Manager will be installed. For example: /opt/IBM/InstallManager

Input Parameters Defined in this Step: Gather Parameters for WebSphere and Deployment Manager, continued

Parameter Name	Default Value	Required	Description
License Acceptance	false	required	Acknowledges that the end user agrees to the IBM International Program License Agreement. This is set to false by default and must be set to true in order for the installation to continue.
Node Name	no default	required	Unique node name that cannot contain any of the following special characters / \ * , ; : = + ? < > & % ' " [] # \$ ^ { }. If you plan to federate into an existing cell later, make sure that the name is unique within that cell.
Profile Name	no default	required	A unique profile name. It cannot begin with a period (.) and cannot contain any of the following special characters / \ * , ; : = + ? < > & % ' " [] # \$ ^ { }.
Web Service Password	no default	required	Password for the discovery web service API.
Web Service User	no default	required	User capable of modifying the managed environment through the discovery web service API.
WebSphere Binary Download Location	/opt/IBM/WAS	required	Fully qualified path to the compressed WebSphere software package on the target machine.
WebSphere Binary Files	no default	required	Comma separated list of file names of the compressed WebSphere software packages.
WebSphere Extract Location	no default	required	Fully qualified path where the compressed software will be extracted on the target machine. This location cannot be the same as Install Manager Extract Location.
WebSphere Install Location	no default	required	Fully qualified path where WebSphere will be installed.
Windows Administrator Password	no default	required	The Windows Administrator password. Required for Windows.
Windows Administrator User	no default	required	This is the Windows Administrator user. Required for Windows.

Additional Input Parameters Defined in this Step: Gather Advanced Parameters for WebSphere and Deployment Manager

Parameter Name	Default Value	Required	Description
Cleanup on Failure	True	optional	Indicates whether to remove downloaded and extracted files and to clean up the installation directory in the event of workflow failure. Valid values are True and False. The default is True, which will clean up on failure.
Cleanup on	True	optional	Indicates whether to remove downloaded and extracted files

Additional Input Parameters Defined in this Step: Gather Advanced Parameters for WebSphere and Deployment Manager, continued

Parameter Name	Default Value	Required	Description
Success			and to clean up the installation directory in the event of workflow success. Valid values are True and False. The default is True, which will clean up on success.
Default Ports	false	optional	Provides the option to assign default ports to a profile. Valid values are true or false. If true, the WebSphere Application Server default ports will be used, and the Ports File and Starting Port parameters should not have values. If false, the workflow will increment the default port until it finds a free port. The default value is false.
Keystore Password	no default	optional	Sets the password for all keystore files created during profile creation. This includes keystore files for both the default personal certificate and the root signing certificate.
Omit Action	no default	optional	Enables you to prevent certain optional features from being installed. Valid values are deployAdminConsole or defaultAppDeployAndConfig. You may only specify one of these options.
Personal CertDN	no default	optional	Distinguished name of the personal certificate. For example: CN=dmlab-example.com,OU=WAS7LabCell,OU=WAS7LabDmgrManager,O=IBM,C=US The DN string cannot contain spaces. If you do not specify the DN, the WebSphere Application Server installer will create one.
Personal CertValidity Period	1	optional	Amount of time in years that the personal certificate is valid. Default is one year.
Ports File	no default	optional	Fully qualified path to a file that defines port settings for the new profile. This file must contain key=value pairs that specify a service name and a port number (for example: WC_adminhost=9060). This option should be used with the Validate Ports option.
Profile Response File	no default	optional	Fully qualified path where the response file that this workflow creates will be located. This file will then be used to drive the installation.
Response File	no default	optional	Fully qualified path where the response file that this workflow creates will be located. This file will then be used to drive the installation and profile creation.
Signing CertDN	no default	optional	Distinguished name of the signing certificate. For example: CN=dmlab-example.com, OU=Root Certificate, OU=WAS7TestLabCell, OU=WAS7LabNode1, O=IBM, C=US The DN string cannot contain spaces. If you do not specify the DN, the WebSphere Application Server installer will create one.

Additional Input Parameters Defined in this Step: Gather Advanced Parameters for WebSphere and Deployment Manager, continued

Parameter Name	Default Value	Required	Description
Signing CertValidity Period	15	optional	Amount of time in years that the root certificate is valid. Default is 15 years.
Starting Port	no default	optional	Starting port number that the profile will use to generate and assign port values. Port values are assigned sequentially from the Starting Port. Do not specify this parameter if you specify Default Ports or Ports File.
Validate Ports	no default	optional	Indicates that the ports should be validated to ensure that they are not already in use. Valid values are true or false. You should use this option if you specify a Ports File.

Provision WebSphere and Stand-Alone

Use this workflow to install the WebSphere 8.0 or 8.5.x Base core binaries and, optionally, create a stand-alone profile.

A stand-alone application server works independently—it is not part of a cell and does not interact with a deployment manager. The stand-alone profile is not suitable for distributed application server environments.

To use this workflow in your environment, see the following information:

Topic	Information Included
"Prerequisites for this Workflow"	List of prerequisites that must be satisfied before you can run this workflow
"How this Workflow Works"	Information about what the workflow does, including validation checks performed, steps executed, and a high-level process flow
"How to Run this Workflow"	Instructions for running this workflow in your environment
"Sample Scenario"	Examples of typical parameter values for this workflow
Parameters	List of input parameters for this workflow

Note: The documentation for this workflow contains steps that are referred to by their base names. The names in the DMA user interface may have a version appended, for example, v2.

Prerequisites for this Workflow

Be sure that the following prerequisites are satisfied before you run the Provision WebSphere and Stand-Alone

workflow:

1. This workflow requires unchallenged sudo access to a user (typically root) who can access all required files and directories.
2. Per the IBM WebSphere 8 documentation, the following system libraries are required before provisioning IBM WebSphere Application Server Network Deployment version 8.0 or 8.5.x on 64-bit and 32-bit Red Hat Linux targets:

Platform	Required Library
64-bit Red Hat Enterprise Linux version 5	<p> compat-libstdc++-33-3.2.3-61 compat-db-4.2.52-5.1 gtk2-2.10.4-29.el5 gtk2-engines-2.8.0-3.el5 ksh-20080202-14 libXp-1.0.0-8 libXmu-1.0.2-5 libXtst-1.0.1-3.1 pam-0.99.6.2-3.26.el5 elfutils-0.125-3.el5 elfutils-libs-0.125-3.el5 libXft-2.1.10-1.1 libstdc++-4.1.2-48 </p> <p> If the target server supports both 32-bit and 64-bit applications then both the 32-bit and 64-bit versions of the following libraries are required: </p> <p> compat-libstdc++-33-3.2.3-61 compat-db-4.2.52-5.1 gtk2-2.18.9-4 gtk2-engines-2.18.4-5 libstdc++-4.1.2-48 libXft-2.1.10-1.1 libXp-1.0.0-8 libXmu-1.0.2-5 libXtst-1.0.1-3.1 pam-0.99.6.2-3.26.el5 </p>
64-bit Red Hat Enterprise Linux version 6	<p> compat-libstdc++-33-3.2.3-69 compat-db-4.6.21-15 ksh-20100621-2 gtk2-2.18.9-4 gtk2-engines-2.18.4-5 libXp-1.0.0-15.1 </p>

Platform	Required Library
	libXmu-1.0.5-1 libXtst-1.0.99.2-3 pam-1.1.1-4 elfutils-0.148-1 elfutils-libs-0.148-1 libXft-2.1.13-4.1 libstdc++-4.4.4-13 If the target server supports both 32-bit and 64-bit applications then both the 32-bit and 64-bit versions of the following libraries are required: compat-libstdc++-33-3.2.3-69 compat-db-4.6.21-15 libstdc++-4.4.4-13 libXp-1.0.0-15.1 libXmu-1.0.5-1 libXtst-1.0.99.2-3 pam-1.1.1-4 libXft-2.1.13-4.1 gtk2-2.18.9-4 gtk2-engines-2.18.4-5

Make sure that these libraries exist on each target server before running this workflow. If newer versions of these libraries are available, you can install the newer versions.

3. This workflow will install WebSphere Application Server as root because of the following IBM documented limitations:
 - Creation of a Linux service for WebSphere Application Server
 - Native registration with the operating system
 - Port conflicts that may occur with other installations of WebSphere Application Server that are not registered with the operating system

If there is a need to run as a non-root user after installation, you can run a recursive `chown` under the installation root and set owner permissions accordingly.

For more information about prerequisites for WebSphere 8, refer to the [WebSphere 8 Product Documentation](#).

How this Workflow Works

This topic contains the following information about the ["Provision WebSphere and Stand-Alone"](#) workflow:

Overview

This workflow does the following three things in the order shown:

1. Installs the IBM Install Manager
2. Installs IBM WebSphere Application Server Network Deployment version 8.0 or 8.5.x
3. Creates a stand-alone profile

The workflow checks to see if the WebSphere 8.0 or 8.5.x binary archive files exist on the target machine. If they do not, the files are downloaded from the software repository.

See the following topics for detailed information:

[Validation Checks Performed](#)

[Steps in this Workflow](#)

[Process Flow](#)

Note: This workflow has been updated to account for the significant changes in the way that WebSphere 8 are installed.

Validation Checks Performed

Most of the validation centers on special characters and spaces in the parameters. There are also validation checks that happen at the operating system level, including file system space checks and RPM checks (on Red Hat Linux platforms only).

The workflow first performs the following parameter checks:

1. Required parameters have values specified.
2. WebSphere specific names do not contain the following characters: `/ \ * , ; = + ? | < > & % ' " [] # $ ^ { }`
3. Parameters do not contain illegal characters for the parameter type.
4. Flag parameters are set to true or false.
5. Integer parameters are set to appropriate integer values.
6. Mutually dependent parameters are specified appropriately as a set.
7. Parameters are set to one of the values if the parameter has a list of valid values.
8. License Acceptance is true (for workflows that input the License Acceptance parameter).
9. All specified file names are legal file names.
10. All specified locations are legal path names. If they do not exist they will be created.

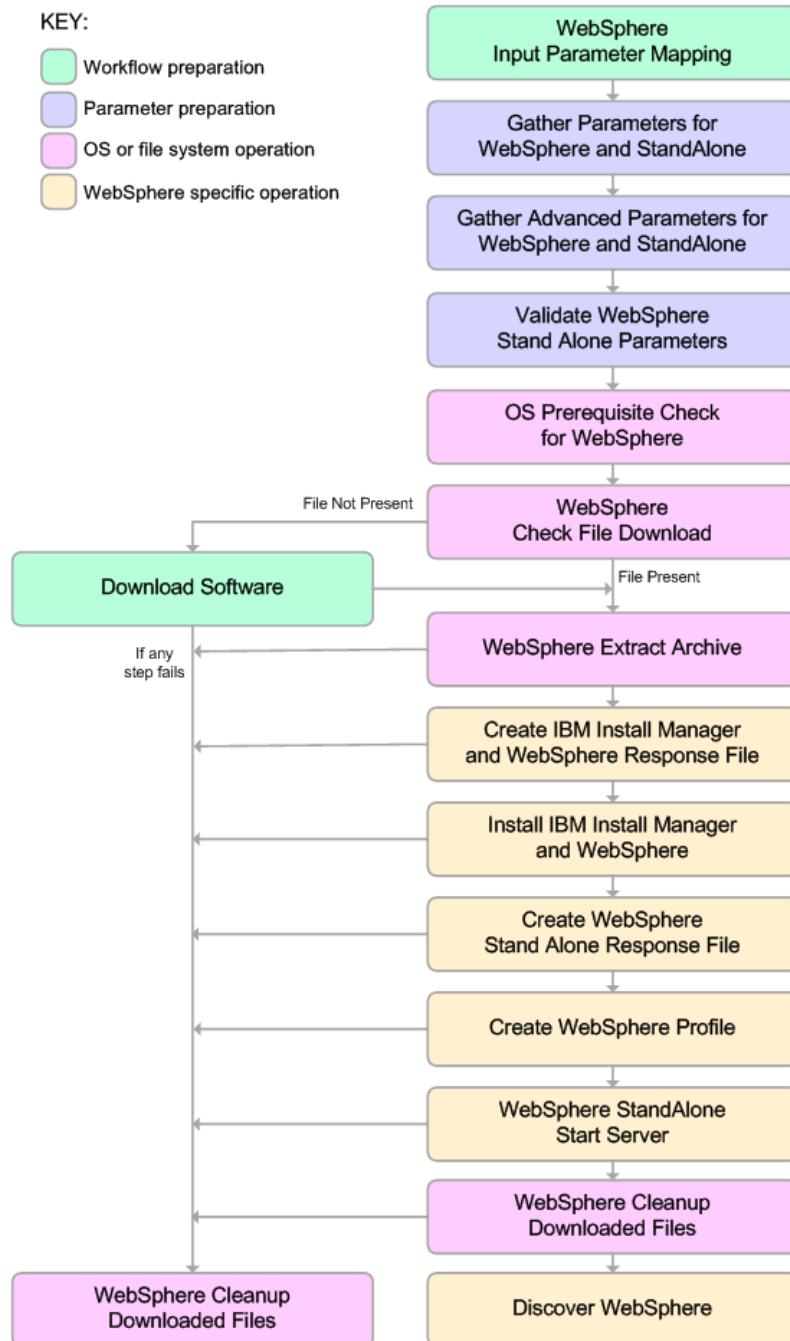
Note: For more information about valid parameter values, see ["Parameters for Provision WebSphere and Stand-Alone"](#).

The workflow then performs the following operating system checks on the target machine:

1. All required libraries are present (see ["Prerequisites for this Workflow"](#) on page 1157).
2. Sufficient disk space is available to install WebSphere 8.0 or 8.5.x.
3. Sufficient disk space is available to extract the binary files from the compressed archive.

Steps Executed

The WebSphere 8.0 or 8.5.x workflow includes the following steps. Each step must complete successfully before the next step can start. If a step fails, the workflow reports a failure, and all subsequent steps are skipped.



Process Flow

This workflow performs the following tasks:

1. Creates the call wrapper and determines the target server platform type.
2. Gathers and validates the parameters needed to install WebSphere 8.0 or 8.5.x and create a stand-alone profile (see ["Validation Checks Performed " on page 1160](#)).
3. Checks the following:
 - a. Documented library requirements for WebSphere 8 (see the ["Prerequisites for this Workflow" on page 1157](#)).
 - b. File system space requirements where WebSphere 8.0 or 8.5.x will be installed.
 - c. Temporary space requirements where the compressed software will be extracted before it is installed.
4. Determines whether the WebSphere 8.0 or 8.5.x binary archive is present on the target machine. If the archive is not present, the workflow downloads it from the software repository.
5. Extracts the WebSphere 8.0 or 8.5.x binary archive to the specified directory.
6. Creates a response file for the purpose of installing a new instance of WebSphere 8.0 or 8.5.x.
7. Installs the IBM Installation Manager and a new WebSphere 8.0 or 8.5.x instance on the target server.
8. Creates a new response file for the purpose of creating a stand-alone profile on top of the WebSphere 8.0 or 8.5.x installation.
9. Creates a stand-alone profile on top of the WebSphere 8.0 or 8.5.x installation.
10. Starts the new stand-alone WebSphere 8.0 or 8.5.x application server.
11. Cleans up any files that were downloaded—for either workflow success or failure.

Note: The parameters Cleanup on Success and Cleanup on Failure are defaulted to True. If they are set to False, the downloaded files are not cleaned up.

12. Discovers any WebSphere 8.0 or 8.5.x cells, clusters, and managed servers associated with the Profile Root that you specify. If these items are found, they are added to the DMA environment.

How to Run this Workflow

The following instructions show you how to customize and run the ["Provision WebSphere and Stand-Alone"](#) workflow in your environment.

The workflow provides default values for some parameters. These default values are usually sufficient for a "typical" installation. You can override the defaults by specifying parameter values in the deployment. You can also expose additional parameters in the workflow, if necessary, to accomplish more advanced scenarios. Any parameters not explicitly specified in the deployment will have the default values listed in ["Parameters for Provision WebSphere and Stand-Alone"](#).

Note: Before following this procedure, review the ["Prerequisites for this Workflow"](#), and ensure that all requirements are satisfied.

To customize and run the Provision WebSphere and Stand-Alone workflow:

1. Create a deployable copy of the workflow.
2. Determine the values that you will specify for the following parameters:

Parameters Defined in this Step: Gather Parameters for WebSphere and StandAlone

Parameter Name	Default Value	Required	Description
Admin Password	no default	optional	When Enable Security is set to true, this parameter must contain a string that does not begin with a dash(-) or contain a space().
Admin User	no default	optional	When Enable Security is set to true, this parameter must contain a string that does not begin with a dash(-), a period(.), or a space(). It cannot contain any of the following characters / \ * , ; = + ? < > & % ' " [] # \$ ^ { }.
Cell Name	no default	required	Unique cell name that does not contain any of the following special characters / \ * , ; = + ? < > & % ' " [] # \$ ^ { }. If you plan to federate into an existing cell later, make sure that this name is not the same as the existing cell name.
Enable Security	no default	required	Enables administrative security. Must be set to either true or false. If Enable Security is true, the Admin User and Admin Password parameters must have values.
Install Manager Binary Download Location	/opt/IBM/iim	required	Fully qualified path to where the compressed Install Manager software package will be downloaded on the target machine. For example: /opt/IBM/iim
Install	no default	required	Name of the compressed Install Manager software

Parameters Defined in this Step: Gather Parameters for WebSphere and StandAlone, continued

Parameter Name	Default Value	Required	Description
Manager Binary Files			package.
Install Manager Extract Location	no default	required	Fully qualified path where the compressed software will be extracted on the target machine. This location cannot be the same as Install Manager Install Location.
Install Manager Install Location	no default	required	Fully qualified path where Install Manager will be installed. For example: /opt/IBM/InstallManager
License Acceptance	false	required	Acknowledges that the end user agrees to the IBM International Program License Agreement. This is set to false by default and must be set to true in order for the installation to continue.
Node Name	no default	required	Unique node name that cannot contain any of the following special characters / \ * , ; = + ? < > & % ' " [] # \$ ^ { }. If you plan to federate into an existing cell later, make sure that the name is unique within that cell.
Profile Name	no default	required	A unique profile name. It cannot begin with a period (.) and cannot contain any of the following special characters / \ * , ; = + ? < > & % ' " [] # \$ ^ { }.
Server Name	no default	required	Name of the application server that will be created under the profile.
Web Service Password	no default	required	Password for the discovery web service API.
Web Service User	no default	required	User capable of modifying the managed environment through the discovery web service API.
WebSphere Binary Download Location	/opt/IBM/WAS	required	Fully qualified path to the compressed WebSphere software package on the target machine.
WebSphere Binary Files	no default	required	Comma separated list of file names of the compressed WebSphere software packages.
WebSphere Extract Location	no default	required	Fully qualified path where the compressed software will be extracted on the target machine. This location cannot be the same as Install Manager Extract Location.
WebSphere Install	no default	required	Fully qualified path where WebSphere will be installed.

Parameters Defined in this Step: Gather Parameters for WebSphere and StandAlone, continued

Parameter Name	Default Value	Required	Description
Location			
Windows Administrator Password	no default	required	The Windows Administrator password. Required for Windows.
Windows Administrator User	no default	required	This is the Windows Administrator user. Required for Windows.

Note: This is the minimum set of parameters required to run this workflow. You may need to expose additional parameters depending on your provisioning objectives.

See ["Parameters for Provision WebSphere and Stand-Alone"](#) for detailed descriptions of all input parameters for this workflow, including default values.

Tip: To avoid having to re-enter passwords whenever they change, you can create a policy to provide them to the workflow.

3. In the workflow editor, expose any additional parameters that you need. You will specify values for those parameters when you create the deployment.
4. Save the changes to the workflow (click **Save** in the lower right corner).
5. Create a new deployment.
6. On the Parameters tab, specify values for the required parameters listed in step 2 and any additional parameters that you have exposed. You do not need to specify values for those parameters whose default values are appropriate for your environment.
7. On the Targets tab, specify one or more targets for this deployment.
8. Save the deployment (click **Save** in the lower right corner).
9. Run the workflow using this deployment.

To verify the results:

Be sure to also perform the following steps:

1. After the workflow has completed, run the following command to check the version of WebSphere Application Server that was installed:

```
WAS_ROOT/bin/versionInfo.sh
```

Here, *WAS_ROOT* is the directory where WebSphere 8.0 or 8.5.x is installed. This is the path that you specified in the WebSphere Install Location parameter.

2. Validate that the profile has been created and is running by doing the following:
 - a. View the *WAS_ROOT*/profiles/*PROFILE_NAME*/logs/AboutThisProfile.txt file. This file is created after the creation of the profile and contains specific information about the profile.

Here, *PROFILE_NAME* is the name of the profile that you just created. This is the name that you specified in the Profile Name parameter.

- b. Change to the *WAS_ROOT*/profiles/*PROFILE_NAME*/logs/*CELL_NAME* directory, and tail the SystemOut.log file. Look for the following line:

```
Server CELL_NAME open for e-business
```

Here, *CELL_NAME* is the name of the WebSphere 8.0 or 8.5.x cell to which this profile pertains. This is the name that you specified in the Cell Name parameter.

Sample Scenario

This topic shows you typical parameter values used for the ["Provision WebSphere and Stand-Alone"](#) workflow.

Tip: To avoid having to re-enter passwords whenever they change, you can create a policy to provide them to the workflow.

New Install with Stand-Alone Profile – Parameter Value Examples

Parameter Name	Example Value	Description
Admin Password	wasPassWord	When Enable Security is set to true, this parameter must contain a string that does not begin with a dash(-) or contain a space().
Admin User	wasadmin	When Enable Security is set to true, this parameter must contain a string that does not begin with a dash(-), a period (.), or a space(). It cannot contain any of the following characters / \ * , ; ; = + ? < > & % ' " [] # \$ ^ { }.
Cell Name	DevCell	Unique cell name that does not contain any of the following special characters / \ * , ; ; = + ? < > & % ' " [] # \$ ^ { }. If you plan to federate into an existing cell later, make sure that this name is not the same as the existing cell name.
Enable Security	true	Enables administrative security. Must be set to either true or false. If Enable Security is true, the Admin User and Admin Password parameters must have values.
Install Manager Binary Download Location	/opt/IBM/iim	Fully qualified path to where the compressed Install Manager software package will be downloaded on the target machine. For example: /opt/IBM/iim
Install Manager Binary Files	IBM_Install_Manager_Linux.zip	Name of the compressed Install Manager software package.
Install Manager Extract Location	/opt/IBM/iim	Fully qualified path where the compressed software will be extracted on the target machine. This location cannot be the same as WebSphere Extract Location.
Install Manager Install Location	/opt/IBM/installManager	Fully qualified path where Install Manager will be installed. For example: /opt/IBM/InstallManager
License Acceptance	true	Acknowledges that the end user agrees to the IBM International Program License Agreement. This is set to false by default and must be set to true in order for the installation to continue.
Node Name	DevNode	Unique node name that cannot contain any of the following special characters / \ * , ; ; = + ? < > & % ' " [] # \$ ^ { }. If

New Install with Stand-Alone Profile – Parameter Value Examples, continued

Parameter Name	Example Value	Description
		you plan to federate into an existing cell later, make sure that the name is unique within that cell.
Profile Name	standAlone	A unique profile name. It cannot begin with a period (.) and cannot contain any of the following special characters / \ * , : ; = + ? < > & % ' " [] # \$ ^ { }.
Server Name	Server1	Name of the application server that will be created under the profile.
Web Service Password	myWebSvcPwd	Password for the discovery web service API.
Web Service User	JohnDoe	User capable of modifying the managed environment through the discovery web service API.
WebSphere Binary Download Location	/opt/IBM/was	Fully qualified path to the compressed WebSphere software package on the target machine.
WebSphere Binary Files	WAS_V8.0_disk1.zip, WAS_V8.0_disk2.zip	Comma separated list of file names of the compressed WebSphere software packages.
WebSphere Extract Location	/opt/IBM/was	Fully qualified path where the compressed software will be extracted on the target machine. This location cannot be the same as Install Manager Extract Location.
WebSphere Install Location	/opt/IBM/WebSphere/AppServer	Fully qualified path where WebSphere will be installed.

Parameters for Provision WebSphere and Stand-Alone

The following tables describe the required and optional input parameters for this workflow. Most of these parameters are not initially visible in a deployment. For most parameters, if you do not specify a value for a parameter, a default value is assigned.

Input Parameters Defined in this Step: Gather Parameters for WebSphere and StandAlone

Parameter Name	Default Value	Required	Description
Admin Password	no default	optional	When Enable Security is set to true, this parameter must contain a string that does not begin with a dash(-) or contain a space().
Admin User	no default	optional	When Enable Security is set to true, this parameter must contain a string that does not begin with a dash(-), a period(.), or a space(). It cannot contain any of the following characters <code>/ \ * , ; ; = + ? < > & % ' " [] # \$ ^ { }</code> .
Call Wrapper	see description	required	Command that will execute this step (or subsequent steps) as a specific user. Defaults are: UNIX targets: <code>/opt/hp/dma/client/jython.sh</code> running as root Windows targets: <code>jython</code> running as Administrator
Cell Name	no default	required	Unique cell name that does not contain any of the following special characters <code>/ \ * , ; ; = + ? < > & % ' " [] # \$ ^ { }</code> . If you plan to federate into an existing cell later, make sure that this name is not the same as the existing cell name.
Enable Security	no default	required	Enables administrative security. Must be set to either true or false. If Enable Security is true, the Admin User and Admin Password parameters must have values.
Host Name	Server.name	required	Hostname or IP address of the target machine.
Install Manager Binary Download Location	<code>/opt/IBM/iim</code>	required	Fully qualified path to where the compressed Install Manager software package will be downloaded on the target machine. For example: <code>/opt/IBM/iim</code>
Install Manager Binary Files	no default	required	Name of the compressed Install Manager software package.
Install Manager Extract Location	no default	required	Fully qualified path where the compressed software will be extracted on the target machine. This location cannot be the same as WebSphere Extract Location.
Install Manager Install Location	no default	required	Fully qualified path where Install Manager will be installed. For example: <code>/opt/IBM/InstallManager</code>

Input Parameters Defined in this Step: Gather Parameters for WebSphere and StandAlone, continued

Parameter Name	Default Value	Required	Description
License Acceptance	false	required	Acknowledges that the end user agrees to the IBM International Program License Agreement. This is set to false by default and must be set to true in order for the installation to continue.
Node Name	no default	required	Unique node name that cannot contain any of the following special characters / \ * , ; = + ? < > & % ' " [] # \$ ^ { }. If you plan to federate into an existing cell later, make sure that the name is unique within that cell.
Profile Name	no default	required	A unique profile name. It cannot begin with a period (.) and cannot contain any of the following special characters / \ * , ; = + ? < > & % ' " [] # \$ ^ { }.
Server Name	no default	required	Name of the application server that will be created under the profile.
Web Service Password	no default	required	Password for the discovery web service API.
Web Service User	no default	required	User capable of modifying the managed environment through the discovery web service API.
WebSphere Binary Download Location	/opt/IBM/WAS	required	Fully qualified path to the compressed WebSphere software package on the target machine.
WebSphere Binary Files	no default	required	Comma separated list of file names of the compressed WebSphere software packages.
WebSphere Extract Location	no default	required	Fully qualified path where the compressed software will be extracted on the target machine. This location cannot be the same as Install Manager Extract Location.
WebSphere Install Location	no default	required	Fully qualified path where WebSphere will be installed.
Windows Administrator Password	no default	required	The Windows Administrator password. Required for Windows.
Windows Administrator User	no default	required	This is the Windows Administrator user. Required for Windows.

Additional Input Parameters Defined in this Step: Gather Advanced Parameters for WebSphere and StandAlone

Parameter Name	Default Value	Required	Description
Cleanup on Failure	True	optional	Indicates whether to remove downloaded and extracted files and to clean up the installation directory in the event of workflow failure. Valid values are True and False. The default

Additional Input Parameters Defined in this Step: Gather Advanced Parameters for WebSphere and StandAlone, continued

Parameter Name	Default Value	Required	Description
			is True, which will clean up on failure.
Cleanup on Success	True	optional	Indicates whether to remove downloaded and extracted files and to clean up the installation directory in the event of workflow success. Valid values are True and False. The default is True, which will clean up on success.
Default Ports	false	optional	Provides the option to assign default ports to a profile. Valid values are true or false. If true, the WebSphere Application Server default ports will be used, and the Ports File and Starting Port parameters should not have values. If false, the workflow will increment the default port until it finds a free port. The default value is false.
Developer Server	no default	optional	Use this parameter for development environments only to help with start up time. Valid value is true. Do not use in production environments.
Keystore Password	no default	optional	Sets the password for all keystore files created during profile creation. This includes keystore files for both the default personal certificate and the root signing certificate.
Omit Action	no default	optional	Enables you to prevent certain optional features from being installed. Valid values are deployAdminConsole or defaultAppDeployAndConfig. You may only specify one of these options.
Personal CertDN	no default	optional	Distinguished name of the personal certificate. For example: CN=dmlab-example.com,OU=WAS7LabCell,OU=WAS7LabDmgrManager,O=IBM,C=US The DN string cannot contain spaces. If you do not specify the DN, the WebSphere Application Server installer will create one.
Personal CertValidity Period	1	optional	Amount of time in years that the personal certificate is valid. Default is one year.
Ports File	no default	optional	Fully qualified path to a file that defines port settings for the new profile. This file must contain key=value pairs that specify a service name and a port number (for example: WC_adminhost=9060). This option should be used with the Validate Ports option.
Profile Response File	no default	optional	Fully qualified path where the response file that this workflow creates will be located. This file will then be used to drive the installation.
Response File	no default	optional	Fully qualified path where the response file that this workflow creates will be located. This file will then be used to drive the installation and profile creation.
Signing CertDN	no default	optional	Distinguished name of the signing certificate. For example: CN=dmlab-example.com, OU=Root Certificate,

Additional Input Parameters Defined in this Step: Gather Advanced Parameters for WebSphere and StandAlone, continued

Parameter Name	Default Value	Required	Description
			OU=WAS7TestLabCell, OU=WAS7LabNode1, O=IBM, C=US The DN string cannot contain spaces. If you do not specify the DN, the WebSphere Application Server installer will create one.
Signing CertValidity Period	15	optional	Amount of time in years that the root certificate is valid. Default is 15 years.
Starting Port	no default	optional	Starting port number that the profile will use to generate and assign port values. Port values are assigned sequentially from the Starting Port. Do not specify this parameter if you specify Default Ports or Ports File.
Validate Ports	no default	optional	Indicates that the ports should be validated to ensure that they are not already in use. Valid values are true or false. You should use this option if you specify a Ports File.

Provision WebSphere Stand-Alone Profile From Existing Install

Use this workflow to create a stand-alone profile on an existing WebSphere 8.0 or 8.5.x installation.

A stand-alone application server works independently—it is not part of a cell and does not interact with a deployment manager. The stand-alone profile is not suitable for distributed application server environments.

To use this workflow in your environment, see the following information:

Topic	Information Included
"Prerequisites for this Workflow"	List of prerequisites that must be satisfied before you can run this workflow
"How this Workflow Works"	Information about what the workflow does, including validation checks performed, steps executed, and a high-level process flow
"How to Run this Workflow"	Instructions for running this workflow in your environment
"Sample Scenario"	Examples of typical parameter values for this workflow
Parameters	List of input parameters for this workflow

Prerequisites for this Workflow

Be sure that the following prerequisites are satisfied before you run the Provision WebSphere Stand-Alone Profile From Existing Install

workflow:

1. This workflow requires unchallenged sudo access to a user (typically root) who can access all required files and directories.
2. Per the IBM WebSphere 8 documentation, the following system libraries are required before provisioning IBM WebSphere Application Server Network Deployment version 8.0 or 8.5.x on 64-bit and 32-bit Red Hat Linux targets:

Platform	Required Library
64-bit Red Hat Enterprise Linux version 5	<p> compat-libstdc++-33-3.2.3-61 compat-db-4.2.52-5.1 gtk2-2.10.4-29.el5 gtk2-engines-2.8.0-3.el5 ksh-20080202-14 libXp-1.0.0-8 libXmu-1.0.2-5 libXtst-1.0.1-3.1 pam-0.99.6.2-3.26.el5 elfutils-0.125-3.el5 elfutils-libs-0.125-3.el5 libXft-2.1.10-1.1 libstdc++-4.1.2-48 </p> <p> If the target server supports both 32-bit and 64-bit applications then both the 32-bit and 64-bit versions of the following libraries are required: </p> <p> compat-libstdc++-33-3.2.3-61 compat-db-4.2.52-5.1 gtk2-2.18.9-4 gtk2-engines-2.18.4-5 libstdc++-4.1.2-48 libXft-2.1.10-1.1 libXp-1.0.0-8 libXmu-1.0.2-5 libXtst-1.0.1-3.1 pam-0.99.6.2-3.26.el5 </p>
64-bit Red Hat Enterprise Linux version 6	<p> compat-libstdc++-33-3.2.3-69 compat-db-4.6.21-15 ksh-20100621-2 gtk2-2.18.9-4 gtk2-engines-2.18.4-5 libXp-1.0.0-15.1 </p>

Platform	Required Library
	libXmu-1.0.5-1 libXtst-1.0.99.2-3 pam-1.1.1-4 elfutils-0.148-1 elfutils-libs-0.148-1 libXft-2.1.13-4.1 libstdc++-4.4.4-13 If the target server supports both 32-bit and 64-bit applications then both the 32-bit and 64-bit versions of the following libraries are required: compat-libstdc++-33-3.2.3-69 compat-db-4.6.21-15 libstdc++-4.4.4-13 libXp-1.0.0-15.1 libXmu-1.0.5-1 libXtst-1.0.99.2-3 pam-1.1.1-4 libXft-2.1.13-4.1 gtk2-2.18.9-4 gtk2-engines-2.18.4-5

Make sure that these libraries exist on each target server before running this workflow. If newer versions of these libraries are available, you can install the newer versions.

3. This workflow will install WebSphere Application Server as root because of the following IBM documented limitations:
 - Creation of a Linux service for WebSphere Application Server
 - Native registration with the operating system
 - Port conflicts that may occur with other installations of WebSphere Application Server that are not registered with the operating system

If there is a need to run as a non-root user after installation, you can run a recursive `chown` under the installation root and set owner permissions accordingly.

For more information about prerequisites for WebSphere 8, refer to the [WebSphere 8 Product Documentation](#).

How this Workflow Works

This topic contains the following information about the "[Provision WebSphere Stand-Alone Profile From Existing Install](#)" workflow:

Overview

This workflow creates a stand-alone profile on an existing WebSphere 8.0 or 8.5.x installation.

See the following topics for detailed information:

[Validation Checks Performed](#)

[Steps in this Workflow](#)

[Process Flow](#)

Validation Checks Performed

Most of the validation centers on special characters and spaces in the parameters. There are also validation checks that happen at the operating system level, including file system space checks and RPM checks (on Red Hat Linux platforms only).

The workflow first performs the following parameter checks:

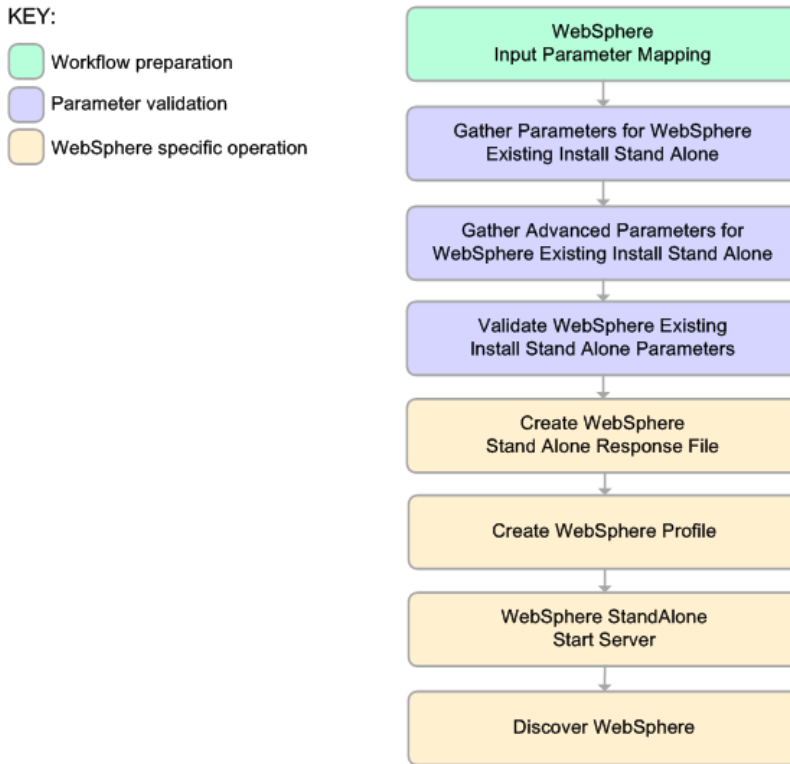
1. Required parameters have values specified.
2. WebSphere specific names do not contain the following characters: / \ * , ; = + ? | < > & % ' " [] # \$ ^ { }
3. Parameters do not contain illegal characters for the parameter type.
4. Flag parameters are set to true or false.
5. Integer parameters are set to appropriate integer values.
6. Mutually dependent parameters are specified appropriately as a set.
7. Parameters are set to one of the values if the parameter has a list of valid values.
8. License Acceptance is true (for workflows that input the License Acceptance parameter).
9. All specified file names are legal file names.
10. All specified locations are legal path names. If they do not exist they will be created.

Note: For more information about valid parameter values, see ["Parameters for Provision WebSphere Stand-Alone Profile from Existing Install"](#).

The workflow then checks to make sure that all required libraries are present on the target machine (see ["Prerequisites for this Workflow"](#)).

Steps Executed

The Provision WebSphere Stand-Alone Profile From Existing Install workflow includes the following steps. Each step must complete successfully before the next step can start. If a step fails, the workflow reports a failure, and all subsequent steps are skipped.



Process Flow

This workflow performs the following tasks:

1. Creates the call wrapper and determines the target server platform type.
2. Gathers and validates the parameters needed to create a stand-alone profile (see "[Validation Checks Performed](#)" on the previous page).
3. Creates a new response file for the purpose of creating a stand-alone profile on top of the existing WebSphere 8.0 or 8.5.x installation.
4. Creates a stand-alone profile on top of the WebSphere 8.0 or 8.5.x installation.
5. Starts the stand-alone application server.
6. Discovers any WebSphere 8.0 or 8.5.x cells, clusters, and managed servers associated with the Profile Root that you specify. If these items are found, they are added to the DMA environment.

How to Run this Workflow

The following instructions show you how to customize and run the ["Provision WebSphere Stand-Alone Profile From Existing Install"](#) workflow in your environment.

The workflow provides default values for some parameters. These default values are usually sufficient for a "typical" installation. You can override the defaults by specifying parameter values in the deployment. You can also expose additional parameters in the workflow, if necessary, to accomplish more advanced scenarios. Any parameters not explicitly specified in the deployment will have the default values listed in ["Parameters for Provision WebSphere Stand-Alone Profile from Existing Install"](#).

Note: Before following this procedure, review the ["Prerequisites for this Workflow"](#), and ensure that all requirements are satisfied.

To customize and run the Provision WebSphere Stand-Alone Profile From Existing Install workflow:

1. Create a deployable copy of the workflow.
2. Determine the values that you will specify for the following parameters:

Parameters Defined in this Step: Gather Parameters for WebSphere Existing Install Stand Alone

Parameter Name	Default Value	Required	Description
Admin Password	no default	optional	When Enable Security is set to true, this parameter must contain a string that does not begin with a dash(-) or contain a space().
Admin User	no default	optional	When Enable Security is set to true, this parameter must contain a string that does not begin with a dash(-), a period(.), or a space(). It cannot contain any of the following characters / \ * , ; : = + ? < > & % ' " [] # \$ ^ { }.
Cell Name	no default	required	Unique cell name that does not contain any of the following special characters / \ * , ; : = + ? < > & % ' " [] # \$ ^ { }. If you plan to federate into an existing cell later, make sure that this name is not the same as the existing cell name.
Enable Security	no default	required	Enables administrative security. Must be set to either true or false. If Enable Security is true, the Admin User and Admin Password parameters must have values.
Node Name	no default	required	Unique node name that cannot contain any of the following special characters / \ * , ; : = + ? < > & % ' " [] # \$ ^ { }. If you plan to federate into an existing cell later, make sure that the name is unique within that cell.

Parameters Defined in this Step: Gather Parameters for WebSphere Existing Install Stand Alone, continued

Parameter Name	Default Value	Required	Description
Profile Name	no default	required	A unique profile name. It cannot begin with a period (.) and cannot contain any of the following special characters / \ * , ; = + ? < > & % ' " [] # \$ ^ { }.
Server Name	no default	required	Name of the application server that will be created under the profile.
Web Service Password	no default	required	Password for the discovery web service API.
Web Service User	no default	required	User capable of modifying the managed environment through the discovery web service API.
WebSphere Install Location	no default	required	Fully qualified path where WebSphere will be installed.
Windows Administrator Password	no default	required	The Windows Administrator password. Required for Windows.
Windows Administrator User	no default	required	This is the Windows Administrator user. Required for Windows.

Note: This is the minimum set of parameters required to run this workflow. You may need to expose additional parameters depending on your provisioning objectives.

See ["Parameters for Provision WebSphere Stand-Alone Profile from Existing Install"](#) for detailed descriptions of all input parameters for this workflow, including default values.

Tip: To avoid having to re-enter passwords whenever they change, you can create a policy to provide them to the workflow.

3. In the workflow editor, expose any additional parameters that you need. You will specify values for those parameters when you create the deployment.
4. Save the changes to the workflow (click **Save** in the lower right corner).
5. Create a new deployment.
6. On the Parameters tab, specify values for the required parameters listed in step 2 and any additional parameters that you have exposed. You do not need to specify values for those parameters whose default values are appropriate for your environment.
7. On the Targets tab, specify one or more targets for this deployment.

8. Save the deployment (click **Save** in the lower right corner).
9. Run the workflow using this deployment.

To verify the results:

The workflow will complete and report SUCCESS on the Console if it has run successfully. If an error occurs during workflow execution, the error is logged, and the workflow terminates in the FAILURE state.

Be sure to also perform the following steps:

1. After the workflow has completed, run the following command to check the version of WebSphere Application Server that was installed:

```
WAS_ROOT/bin/versionInfo.sh
```

Here, *WAS_ROOT* is the directory where WebSphere 8.0 or 8.5.x is installed. This is the path that you specified in the WebSphere Install Location parameter.

2. Validate that the profile has been created and is running by doing the following:
 - a. View the *WAS_ROOT*/profiles/*PROFILE_NAME*/logs/AboutThisProfile.txt file. This file is created after the creation of the profile and contains specific information about the profile.

Here, *PROFILE_NAME* is the name of the profile that you just created. This is the name that you specified in the Profile Name parameter.

- b. Change to the *WAS_ROOT*/profiles/*PROFILE_NAME*/logs/*CELL_NAME* directory, and tail the SystemOut.log file. Look for the following line:

```
Server CELL_NAME open for e-business
```

Here, *CELL_NAME* is the name of the WebSphere 8.0 or 8.5.x cell to which this profile pertains. This is the name that you specified in the Cell Name parameter.

Sample Scenario

This topic shows you typical parameter values used for the ["Provision WebSphere Stand-Alone Profile From Existing Install"](#) workflow.

Tip: To avoid having to re-enter passwords whenever they change, you can create a policy to provide them to the workflow.

Stand-Alone Profile on Existing Install – Parameter Value Examples

Parameter Name	Example Value	Description
Admin Password	wasPassWord	When Enable Security is set to true, this parameter must contain a string that does not begin with a dash(-) or contain a space().
Admin User	wasadmin	When Enable Security is set to true, this parameter must contain a string that does not begin with a dash(-), a period(.), or a space(). It cannot contain any of the following characters / \ * , ; = + ? < > & % ' " [] # \$ ^ { }.
Cell Name	DevStandAlone1Cell	Unique cell name that does not contain any of the following special characters / \ * , ; = + ? < > & % ' " [] # \$ ^ { }. If you plan to federate into an existing cell later, make sure that this name is not the same as the existing cell name.
Enable Security	true	Enables administrative security. Must be set to either true or false. If Enable Security is true, the Admin User and Admin Password parameters must have values.
Node Name	DevStandAlone1Node	Unique node name that cannot contain any of the following special characters / \ * , ; = + ? < > & % ' " [] # \$ ^ { }. If you plan to federate into an existing cell later, make sure that the name is unique within that cell.
Profile Name	StandAlone1	A unique profile name. It cannot begin with a period (.) and cannot contain any of the following special characters / \ * , ; = + ? < > & % ' " [] # \$ ^ { }.
Server Name	Server1	Name of the application server that will be created under the profile.
Web Service Password	myWebSvcPwd	Password for the discovery web service API.
Web Service User	JohnDoe	User capable of modifying the managed environment through the discovery web service API.

Stand-Alone Profile on Existing Install – Parameter Value Examples, continued

Parameter Name	Example Value	Description
WebSphere Install Location	/opt/IBM/ WebSphere/AppServer	Fully qualified path where WebSphere will be installed.

Parameters for Provision WebSphere Stand-Alone Profile from Existing Install

The following tables describe the required and optional input parameters for this workflow. Most of these parameters are not initially visible in a deployment. For most parameters, if you do not specify a value for a parameter, a default value is assigned.

Input Parameters Defined in this Step: Gather Parameters for WebSphere Existing Install Stand Alone

Parameter Name	Default Value	Required	Description
Admin Password	no default	optional	When Enable Security is set to true, this parameter must contain a string that does not begin with a dash(-) or contain a space().
Admin User	no default	optional	When Enable Security is set to true, this parameter must contain a string that does not begin with a dash(-), a period(.), or a space(). It cannot contain any of the following characters / \ * , ; ; = + ? < > & % ' " [] # \$ ^ { }.
Call Wrapper	see description	required	Command that will execute this step (or subsequent steps) as a specific user. Defaults are: UNIX targets: /opt/hp/dma/client/jython.sh running as root Windows targets: jython running as Administrator
Cell Name	no default	required	Unique cell name that does not contain any of the following special characters / \ * , ; ; = + ? < > & % ' " [] # \$ ^ { }. If you plan to federate into an existing cell later, make sure that this name is not the same as the existing cell name.
Enable Security	no default	required	Enables administrative security. Must be set to either true or false. If Enable Security is true, the Admin User and Admin Password parameters must have values.
Host Name	Server.name	required	Hostname or IP address of the target machine.
Node Name	no default	required	Unique node name that cannot contain any of the following special characters / \ * , ; ; = + ? < > & % ' " [] # \$ ^ { }. If you plan to federate into an existing cell later, make sure that the name is unique within that cell.
Profile Name	no default	required	A unique profile name. It cannot begin with a period (.) and cannot contain any of the

Input Parameters Defined in this Step: Gather Parameters for WebSphere Existing Install Stand Alone, continued

Parameter Name	Default Value	Required	Description
			following special characters / \ * , ; = + ? < > & % ' " [] # \$ ^ { }.
Server Name	no default	required	Name of the application server that will be created under the profile.
Web Service Password	no default	required	Password for the discovery web service API.
Web Service User	no default	required	User capable of modifying the managed environment through the discovery web service API.
WebSphere Install Location	no default	required	Fully qualified path where WebSphere will be installed.
Windows Administrator Password	no default	required	The Windows Administrator password. Required for Windows.
Windows Administrator User	no default	required	This is the Windows Administrator user. Required for Windows.

Additional Input Parameters Defined in this Step: Gather Advanced Parameters for WebSphere Existing Install Stand Alone

Parameter Name	Default Value	Required	Description
Default Ports	false	optional	Provides the option to assign default ports to a profile. Valid values are true or false. If true, the WebSphere Application Server default ports will be used, and the Ports File and Starting Port parameters should not have values. If false, the workflow will increment the default port until it finds a free port. The default value is false.
Developer Server	no default	optional	Use this parameter for development environments only to help with start up time. Valid value is true. Do not use in production environments.
Keystore Password	no default	optional	Sets the password for all keystore files created during profile creation. This includes keystore files for both the default personal certificate and the root signing certificate.
Omit Action	no default	optional	Enables you to prevent certain optional features from being installed. Valid values are deployAdminConsole or defaultAppDeployAndConfig. You may only specify one of these options.
Personal CertDN	no default	optional	Distinguished name of the personal certificate. For example: CN=dmalab-example.com,OU=WAS7LabCell,

Additional Input Parameters Defined in this Step: Gather Advanced Parameters for WebSphere Existing Install Stand Alone, continued

Parameter Name	Default Value	Required	Description
			OU=WAS7LabDmgrManager,O=IBM,C=US The DN string cannot contain spaces. If you do not specify the DN, the WebSphere Application Server installer will create one.
Personal CertValidity Period	1	optional	Amount of time in years that the personal certificate is valid. Default is one year.
Ports File	no default	optional	Fully qualified path to a file that defines port settings for the new profile. This file must contain key=value pairs that specify a service name and a port number (for example: WC_adminhost=9060). This option should be used with the Validate Ports option.
Profile Response File	no default	optional	Fully qualified path where the response file that this workflow creates will be located. This file will then be used to drive the installation.
Signing CertDN	no default	optional	Distinguished name of the signing certificate. For example: CN=dmalab-example.com, OU=Root Certificate, OU=WAS7TestLabCell, OU=WAS7LabNode1, O=IBM, C=US The DN string cannot contain spaces. If you do not specify the DN, the WebSphere Application Server installer will create one.
Signing CertValidity Period	15	optional	Amount of time in years that the root certificate is valid. Default is 15 years.
Starting Port	no default	optional	Starting port number that the profile will use to generate and assign port values. Port values are assigned sequentially from the Starting Port. Do not specify this parameter if you specify Default Ports or Ports File.
Validate Ports	no default	optional	Indicates that the ports should be validated to ensure that they are not already in use. Valid values are true or false. You should use this option if you specify a Ports File.

WebSphere - Provision IBM HTTP Server

Use this workflow to install IBM HTTP Server for WebSphere Application Server version 8.0 or 8.5.x and the plug-in on a target system and then to configure a Web server instance along with the plug-in on the same target system.

IBM HTTP Server version 8.0 or 8.5.x is a Web server that will serve both static and dynamic content. Usually you will front your WebSphere Application Server environment with an IBM HTTP Server.

To use this workflow in your environment, see the following information:

Topic	Information Included
"Prerequisites for this Workflow"	List of prerequisites that must be satisfied before you can run this workflow
"How this Workflow Works"	Information about what the workflow does, including validation checks performed, steps executed, and a high-level process flow
"How to Run this Workflow"	Instructions for running this workflow in your environment
"Sample Scenario"	Examples of typical parameter values for this workflow
Parameters	List of input parameters for this workflow

Note: The documentation for this workflow contains steps that are referred to by their base names. The names in the DMA user interface may have a version appended, for example, v2.

Prerequisites for this Workflow

Be sure that the following prerequisites are satisfied before you run the WebSphere - Configure IBM HTTP Server workflow:

1. This workflow requires unchallenged `sudo` access to a user (typically `root`) who can access all required files and directories.
2. Per the IBM WebSphere 8 documentation, the following system libraries are required before provisioning IBM WebSphere Application Server Network Deployment version 8.0 or 8.5.x on 64-bit and 32-bit Red Hat Linux targets:

Platform	Required Library
64-bit Red Hat Enterprise Linux version 5	compat-libstdc++-33-3.2.3-61 compat-db-4.2.52-5.1 gtk2-2.10.4-29.el5 gtk2-engines-2.8.0-3.el5 ksh-20080202-14 libXp-1.0.0-8 libXmu-1.0.2-5 libXtst-1.0.1-3.1 pam-0.99.6.2-3.26.el5 elfutils-0.125-3.el5 elfutils-libs-0.125-3.el5 libXft-2.1.10-1.1 libstdc++-4.1.2-48 <div> If the target server supports both 32-bit and 64-bit applications then both the 32-bit and 64-bit versions of the following libraries are required: </div> compat-libstdc++-33-3.2.3-61 compat-db-4.2.52-5.1 gtk2-2.18.9-4 gtk2-engines-2.18.4-5 libstdc++-4.1.2-48 libXft-2.1.10-1.1 libXp-1.0.0-8 libXmu-1.0.2-5 libXtst-1.0.1-3.1 pam-0.99.6.2-3.26.el5
64-bit Red Hat Enterprise Linux version 6	compat-libstdc++-33-3.2.3-69 compat-db-4.6.21-15 ksh-20100621-2 gtk2-2.18.9-4 gtk2-engines-2.18.4-5 libXp-1.0.0-15.1 libXmu-1.0.5-1 libXtst-1.0.99.2-3

Platform	Required Library
	<p> pam-1.1.1-4 elfutils-0.148-1 elfutils-libs-0.148-1 libXft-2.1.13-4.1 libstdc++-4.4.4-13 </p> <p> If the target server supports both 32-bit and 64-bit applications then both the 32-bit and 64-bit versions of the following libraries are required: </p> <p> compat-libstdc++-33-3.2.3-69 compat-db-4.6.21-15 libstdc++-4.4.4-13 libXp-1.0.0-15.1 libXmu-1.0.5-1 libXtst-1.0.99.2-3 pam-1.1.1-4 libXft-2.1.13-4.1 gtk2-2.18.9-4 gtk2-engines-2.18.4-5 </p>

Make sure that these libraries exist on each target server before running this workflow. If newer versions of these libraries are available, you can install the newer versions.

For more information about prerequisites for WebSphere 8, refer to the [WebSphere 8 Product Documentation](#).

How this Workflow Works

This topic contains the following information about the ["WebSphere - Provision IBM HTTP Server"](#) workflow:

Overview

This workflow does the following these things in the order shown:

1. Installs the IBM Install Manager
2. Installs IBM HTTP Server version 8.0 or 8.5.x and the plug-in
3. Configures a Web server instance
4. Creates a plug-in configuration for the Web server instance
5. Optionally, creates the HTTP admin instance
6. Optionally, creates Self Signed Certificate for the Web server instance
7. Optionally, runs all Web server instances and the HTTP admin instance as a non-root system account
8. Starts the Web server instance and, if configured, starts the HTTP admin instance
9. Discovers all IBM HTTP Server instances and populates DMA with the relevant configuration information

The workflow checks to see if the IBM HTTP Server version 8.0 or 8.5.x binary archive files exist on the target machine. If they do not, the files are downloaded from the software repository.

Note: This workflow has been updated to account for the significant changes in the way that WebSphere 8 are installed.

Validation Checks Performed

Most of the validation centers on special characters and spaces in the parameters. There are also validation checks that happen at the operating system level, including file system space checks and RPM checks (on Red Hat Linux platforms only).

The workflow first performs the following parameter checks:

1. Required parameters have values specified.
2. WebSphere specific names do not contain the following characters: `/ \ * , ; = + ? | < > & % ' " [] # $ ^ { }`
3. Parameters do not contain illegal characters for the parameter type.
4. Flag parameters are set to true or false.
5. Integer parameters are set to appropriate integer values.
6. Mutually dependent parameters are specified appropriately as a set.
7. Parameters are set to one of the values if the parameter has a list of valid values.
8. License Acceptance is true (for workflows that input the License Acceptance parameter).
9. All specified file names are legal file names.
10. All specified locations are legal path names. If they do not exist they will be created.

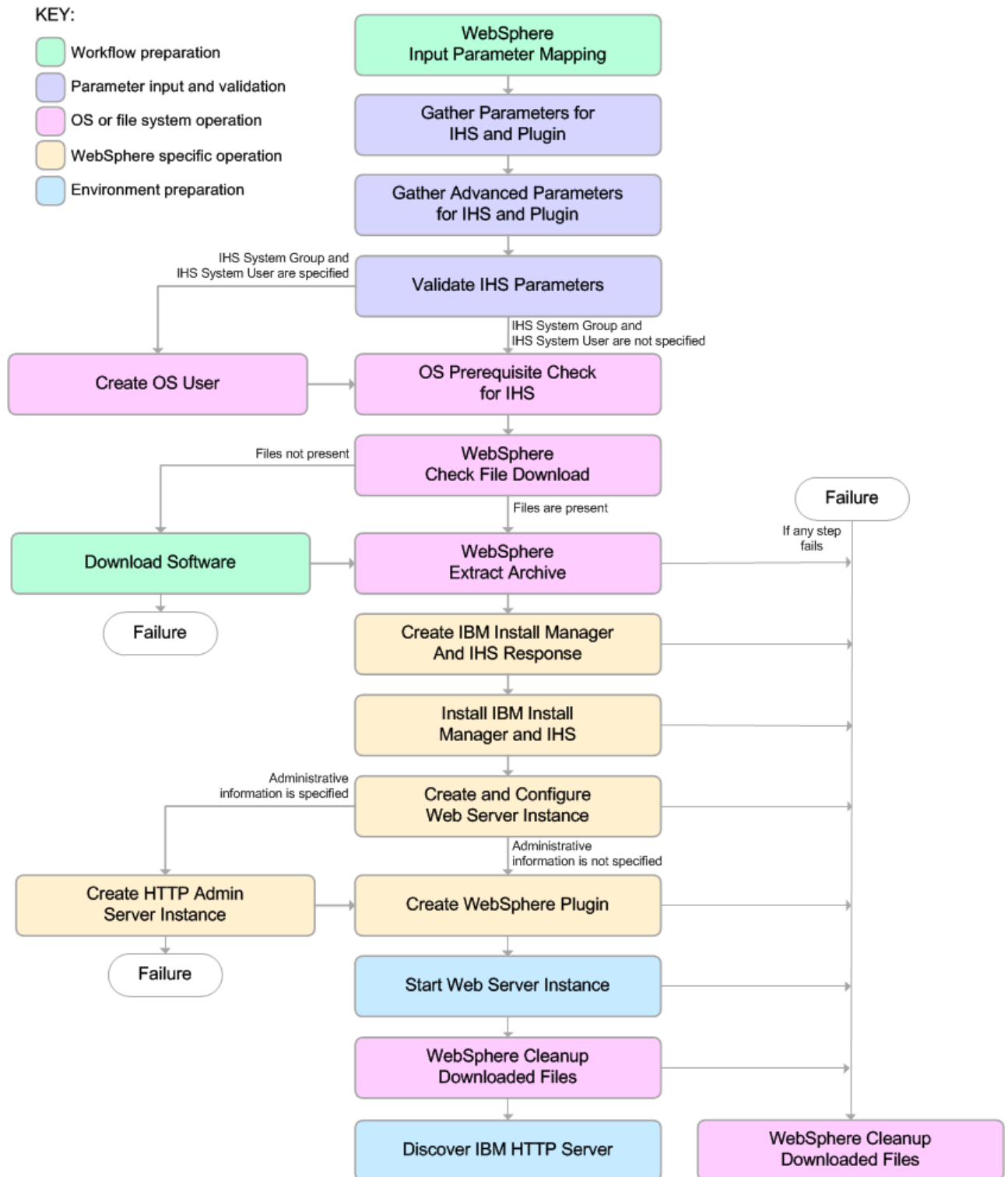
Note: For more information about valid parameter values, see ["Parameters for WebSphere - Provision IBM HTTP Server" on page 1206](#).

The workflow then performs the following operating system checks on the target machine:

1. All required libraries are present (see ["Prerequisites for this Workflow"](#)).
2. Sufficient disk space is available to install IBM HTTP Server for WebSphere Application Server version 8.0 or 8.5.x.
3. Sufficient disk space is available to extract the binary files from the compressed archive.

Steps Executed

The WebSphere - Provision IBM HTTP Server workflow includes the following steps. Each step must complete successfully before the next step can start. If a step fails, the workflow reports a failure, and all subsequent steps are skipped.



Process Flow

This workflow performs the following tasks:

1. Creates the call wrapper to facilitate the execution of subsequent steps.
2. Gathers and validates the parameters needed to install IBM HTTP Server version 8.0 or 8.5.x and the plug-in (see ["Validation Checks Performed " on page 1191](#)).
3. *Optional:* Creates the operating system user—if IHS System User and IHS System Group are specified.
4. Checks the following:
 - a. Documented library requirements for IBM HTTP Server versions 8.0 and 8.5.x (see the ["Prerequisites for this Workflow"](#)).
 - b. File system space requirements where IBM HTTP Server version 8.0 or 8.5.x will be installed.
 - c. Temporary space requirements where the compressed software will be extracted before it is installed.
5. Determines whether the IBM HTTP Server version 8.0 or 8.5.x binary archive and the Install Manager binary archive are present on the target machine. If the files are not present, the workflow downloads them from the software repository.
6. Extracts the IBM HTTP Server version 8.0 or 8.5.x and Install Manager binary archives to the specified directories.
7. Creates a response file for the purpose of installing the IBM Install Manager, a new IBM HTTP Server version 8.0 or 8.5.x instance, and the WebSphere plug-in.
8. Installs the IBM Installation Manager, a new IBM HTTP Server version 8.0 or 8.5.x instance, and the WebSphere plug-in on the target server.
9. Creates a new Web server instance under the installation root of IBM HTTP Server.
10. *Optional:* Creates the HTTP Admin Web server instance—if HTTP Admin User, HTTP Admin Password, and HTTP Admin Port are specified.
11. Creates the plug-in configuration files and plug-in log directory.
12. Starts the Web server instance.
13. Cleans up any files that were downloaded—for either workflow success or failure.

Note: The parameters Cleanup on Success and Cleanup on Failure are defaulted to True. If they are set to False, the downloaded files are not cleaned up.

14. Discovers all IBM HTTP Server instances and populates DMA with the relevant configuration information.

How to Run this Workflow

The following instructions show you how to customize and run the ["WebSphere - Provision IBM HTTP Server"](#) workflow in your environment.

The workflow provides default values for some parameters. These default values are usually sufficient for a "typical" installation. You can override the defaults by specifying parameter values in the deployment. You can also expose additional parameters in the workflow, if necessary, to accomplish more advanced scenarios. Any parameters not explicitly specified in the deployment will have the default values listed in ["Parameters for WebSphere - Provision IBM HTTP Server"](#).

Note: Before following this procedure, review the ["Prerequisites for this Workflow"](#), and ensure that all requirements are satisfied.

To customize and run the WebSphere - Provision IBM HTTP Server workflow:

1. Create a deployable copy of the workflow.
2. Determine the values that you will specify for the following parameters:

Parameters Defined in this Step: Gather Parameters for Provision IBM HTTP Server

Parameter Name	Default Value	Required	Description
Http Port	80	required	The port on which the Web server will listen. Default is set to 80. If the Web server instance is run as non-root this value has to be greater than 1024.
IHS Binary Download Location	no default	required	Fully-qualified path to the compressed IHS software package.
IHS Binary Files	no default	required	Name of the compressed IHS software package.
IHS Extract Location	no default	required	Fully-qualified path where the compressed software will be extracted on the target machine. This cannot be the same as the Install Manager Extract Location.
IHS Install Location	no default	required	Fully-qualified path where IHS will be installed.
Install Manager Binary Download Location	no default	required	Fully-qualified path to the compressed Install Manager software package on the target machine.
Install Manager Binary Files	no default	required	Name of the compressed Install Manager software package.

Parameters Defined in this Step: Gather Parameters for Provision IBM HTTP Server, continued

Parameter Name	Default Value	Required	Description
Install Manager Extract Location	no default	required	Fully-qualified path where the compressed software will be extracted on the target machine. This location cannot be the same as the IHS Extract Location.
Install Manager Install Location	no default	required	Fully-qualified path where the Install Manager will be installed.
License Acceptance	false	required	Acknowledges that the end user agrees to the IBM International Program License Agreement. This is set to false by default and must be set to true for the installation to continue.
Web Server Name	no default	required	Required: Fully-qualified name of the Web server instance. There can be no spaces in the name. For example: <code>myapp.hp.com</code>
Windows Password	no default	required (if Windows)	Windows Administrator password.
Windows Username	no default	required(if Windows)	Windows Administrator username. Domain/Username.

Note: This is the minimum set of parameters required to run this workflow. You may need to expose additional parameters depending on your provisioning objectives.

See ["Parameters for WebSphere - Provision IBM HTTP Server" on page 1206](#) for detailed descriptions of all input parameters for this workflow, including default values.

Tip: To avoid having to re-enter passwords whenever they change, you can create a policy to provide them to the workflow.

3. In the workflow editor, expose any additional parameters that you need. You will specify values for those parameters when you create the deployment.
4. Save the changes to the workflow (click **Save** in the lower right corner).
5. Create a new deployment.
6. On the Parameters tab, specify values for the required parameters listed in step 2 and any additional parameters that you have exposed. You do not need to specify values for those parameters whose default values are appropriate for your environment.
7. On the Targets tab, specify one or more targets for this deployment.

8. Save the deployment (click **Save** in the lower right corner).
9. Run the workflow using this deployment.

To verify the results:

Be sure to also perform the following step:

After the workflow has completed, run the following command to check the version of IBM HTTP Server that was installed:

```
WAS_ROOT/bin/versionInfo.sh
```

Here, *WAS_ROOT* is the directory where IBM HTTP Server was installed. For example:
/opt/IBM/HTTPServer

Sample Scenario

This topic shows you typical parameter values used for the ["WebSphere - Provision IBM HTTP Server"](#) workflow.

Tip: To avoid having to re-enter passwords whenever they change, you can create a policy to provide them to the workflow.

Scenario 1:

Provision IBM HTTP Server 8 and plug-in with root - Parameter Value Examples

Parameter Name	Example Value	Description
Http Port	80	The port on which the Web server will listen. Default is set to 80. If the Web server instance is run as non-root this value has to be greater than 1024.
IHS Binary Download Location	/opt/wasv8	Name of the compressed IHS software package.
IHS Binary Files	IHSbinary1.zip, IHSbinary2.zip, IHSbinary3.zip, IHSbinary4.zip,	Name of the compressed IHS software package.
IHS Extract Location	/opt/ihsv8	Fully-qualified path where the compressed software will be extracted on the target machine. This cannot be the same as the Install Manager Extract Location.
IHS Install Location	/opt/IBM/HTTPServer	Fully-qualified path where IHS will be installed.
Install Manager Binary Download Location	/opt/IBM/iim	Fully-qualified path to the compressed Install Manager software package on the target machine.
Install Manager Binary Files	IBM_Install_Manager_Linux_1.5.3.zip	Name of the compressed Install Manager software package.
Install Manager Extract Location	/opt/IBM/iim	Fully-qualified path where the compressed software will be extracted on the target machine. This location cannot be the same as the IHS Extract Location.
Install Manager Install Location	/opt/IBM/installManager	Fully-qualified path where the Install Manager will be installed.
License Acceptance	true	Acknowledges that the end user agrees to the IBM International Program License Agreement. This is set to false by default and must be set to true for the installation to continue.
Web Server	example.	Required: Fully-qualified name of the Web server

Provision IBM HTTP Server 8 and plug-in with root - Parameter Value Examples, continued

Parameter Name	Example Value	Description
Name	mycompany.com	instance. There can be no spaces in the name. For example: myapp.hp.com
Windows Password	WinPsWd	Password for the Windows Administrator.
Windows Username	Domain/Username	Windows Administrator username.

Scenario 2:**Provision IBM HTTP Server 8 and plug-in with non-root - Parameter Value Examples**

Parameter Name	Example Value	Description
Http Port	80	The port on which the Web server will listen. Default is set to 80. If the Web server instance is run as non-root this value has to be greater than 1024.
IHS Binary Download Location	/opt/wasv8	Name of the compressed IHS software package.
IHS Binary Files	IHSbinary1.zip, IHSbinary2.zip, IHSbinary3.zip, IHSbinary4.zip,	Name of the compressed IHS software package.
IHS Extract Location	/opt/ihsv8	Fully-qualified path where the compressed software will be extracted on the target machine. This cannot be the same as the Install Manager Extract Location.
IHS Install Location	/opt/IBM/HTTPServer	Fully-qualified path where IHS will be installed.
Install Manager Binary Download Location	/opt/IBM/iim	Fully-qualified path to the compressed Install Manager software package on the target machine.
Install Manager Binary Files	IBM_Install_Manager_Linux_1.5.3.zip	Name of the compressed Install Manager software package.
Install Manager Extract Location	/opt/IBM/iim	Fully-qualified path where the compressed software will be extracted on the target machine. This location cannot be the same as the IHS Extract Location.
Install Manager	/opt/IBM/installManager	Fully-qualified path where the Install Manager will be installed.

Provision IBM HTTP Server 8 and plug-in with non-root - Parameter Value Examples, continued

Parameter Name	Example Value	Description
Install Location		
License Acceptance	true	Acknowledges that the end user agrees to the IBM International Program License Agreement. This is set to false by default and must be set to true for the installation to continue.
Web Server Name	example.mycompany.com	Required: Fully-qualified name of the Web server instance. There can be no spaces in the name. For example: myapp.hp.com
Windows Password	WinPsWd	Password for the Windows Administrator.
Windows Username	Domain/Username	Windows Administrator username.
IHS System Group	webadmin	The group that owns and runs the Web server instances and the plug-in directories. If the system group account does not already exist the account will be created on the target machine.
IHS System Password	SysPsWd	The password for the user that owns and runs the Web server instances and the plug-in directories. This password will be used when creating the system user.
IHS System User	ihadmin	The user that owns and runs the Web server instances and the plug-in directories. If the system user account does not already exist the account will be created on the target machine.

Note: For this use case you need to expose the following parameters in the Gather Advanced Parameters for Provision IBM HTTP Server step:

The IHS System parameters: IHS System Group, IHS System Password, and IHS System User

Scenario 3:**Provision IBM HTTP Server 8, plug-in, and HTTP Admin Server with non-root - Parameter Value Examples**

Parameter Name	Example Value	Description
Http Port	80	The port on which the Web server will listen. Default is set to 80. If the Web server instance is run as non-root this value has to be greater than 1024.
IHS Binary Download	/opt/wasv8	Name of the compressed IHS software package.

Provision IBM HTTP Server 8, plug-in, and HTTP Admin Server with non-root - Parameter Value Examples, continued

Parameter Name	Example Value	Description
Location		
IHS Binary Files	IHSbinary1.zip, IHSbinary2.zip, IHSbinary3.zip, IHSbinary4.zip,	Name of the compressed IHS software package.
IHS Extract Location	/opt/ihsv8	Fully-qualified path where the compressed software will be extracted on the target machine. This cannot be the same as the Install Manager Extract Location.
IHS Install Location	/opt/IBM/HTTPServer	Fully-qualified path where IHS will be installed.
Install Manager Binary Download Location	/opt/IBM/iim	Fully-qualified path to the compressed Install Manager software package on the target machine.
Install Manager Binary Files	IBM_Install_Manager_Linux_1.5.3.zip	Name of the compressed Install Manager software package.
Install Manager Extract Location	/opt/IBM/iim	Fully-qualified path where the compressed software will be extracted on the target machine. This location cannot be the same as the IHS Extract Location.
Install Manager Install Location	/opt/IBM/installManager	Fully-qualified path where the Install Manager will be installed.
License Acceptance	true	Acknowledges that the end user agrees to the IBM International Program License Agreement. This is set to false by default and must be set to true for the installation to continue.
Web Server Name	example. mycompany.com	Required: Fully-qualified name of the Web server instance. There can be no spaces in the name. For example: myapp.hp.com
Web Service Password	WebSrvPsWd	Password for the discovery web service API.
Web Service User	no default	User capable of modifying the managed environment through the discovery web service API.
HTTP Admin Password	AdMinPsWd	Password for the HTTP Admin User. If specified, HTTP Admin Port and HTTP Admin User must also be specified. If not specified, HTTP Admin Port and HTTP Admin User must not be specified.

Provision IBM HTTP Server 8, plug-in, and HTTP Admin Server with non-root - Parameter Value Examples, continued

Parameter Name	Example Value	Description
HTTP Admin Port	8004	Port of the IBM HTTP Server administrative server. If specified, HTTP Admin Password and HTTP Admin User must also be specified. If not specified, HTTP Admin Password and HTTP Admin User must not be specified.
HTTP Admin User	wasadmin	User name of the IBM HTTP administrative user. If specified, HTTP Admin Password and HTTP Admin Port must also be specified. If not specified, HTTP Admin Password and HTTP Admin Port must not be specified.
IHS System Group	webadmin	The group that owns and runs the Web server instances and the plug-in directories. If the system group account does not already exist the account will be created on the target machine.
IHS System Password	SysPsWd	The password for the user that owns and runs the Web server instances and the plug-in directories. This password will be used when creating the system user.
IHS System User	ihsadmin	The user that owns and runs the Web server instances and the plug-in directories. If the system user account does not already exist the account will be created on the target machine.

Note: For this use case you need to expose the following parameters in the Gather Advanced Parameters for Provision IBM HTTP Server step:

- The IHS System parameters: IHS System Group, IHS System Password, and IHS System User
- The HTTP Admin parameters: HTTP Admin Password, HTTP Admin Port, and HTTP Admin User

Scenario 4:

Provision IBM HTTP Server 8, plug-in, HTTP Admin Server, and HTTP SSL with non-root - Parameter Value Examples

Parameter Name	Example Value	Description
Http Port	80	The port on which the Web server will listen. Default is set to 80. If the Web server instance is run as non-root this value has to be greater than 1024.
IHS Binary Download Location	/opt/wasv8	Name of the compressed IHS software package.

Provision IBM HTTP Server 8, plug-in, HTTP Admin Server, and HTTP SSL with non-root - Parameter Value Examples, continued

Parameter Name	Example Value	Description
IHS Binary Files	IHSbinary1.zip, IHSbinary2.zip, IHSbinary3.zip, IHSbinary4.zip,	Name of the compressed IHS software package.
IHS Extract Location	/opt/ihsv8	Fully-qualified path where the compressed software will be extracted on the target machine. This cannot be the same as the Install Manager Extract Location.
IHS Install Location	/opt/IBM/HTTPServer	Fully-qualified path where IHS will be installed.
Install Manager Binary Download Location	/opt/IBM/iim	Fully-qualified path to the compressed Install Manager software package on the target machine.
Install Manager Binary Files	IBM_Install_Manager_Linux_1.5.3.zip	Name of the compressed Install Manager software package.
Install Manager Extract Location	/opt/IBM/iim	Fully-qualified path where the compressed software will be extracted on the target machine. This location cannot be the same as the IHS Extract Location.
Install Manager Install Location	/opt/IBM/installManager	Fully-qualified path where the Install Manager will be installed.
License Acceptance	true	Acknowledges that the end user agrees to the IBM International Program License Agreement. This is set to false by default and must be set to true for the installation to continue.
Web Server Name	example. mycompany.com	Required: Fully-qualified name of the Web server instance. There can be no spaces in the name. For example: myapp.hp.com
Web Service Password	WebSrvPsWd	Password for the discovery web service API.
Web Service User	no default	User capable of modifying the managed environment through the discovery web service API.
HTTP Admin Password	AdMinPsWd	Password for the HTTP Admin User. If specified, HTTP Admin Port and HTTP Admin User must also be specified. If not specified, HTTP Admin Port and HTTP Admin User must not be specified.
HTTP	8004	Port of the IBM HTTP Server administrative server. If

Provision IBM HTTP Server 8, plug-in, HTTP Admin Server, and HTTP SSL with non-root - Parameter Value Examples, continued

Parameter Name	Example Value	Description
Admin Port		specified, HTTP Admin Password and HTTP Admin User must also be specified. If not specified, HTTP Admin Password and HTTP Admin User must not be specified.
HTTP Admin User	wasadmin	User name of the IBM HTTP administrative user. If specified, HTTP Admin Password and HTTP Admin Port must also be specified. If not specified, HTTP Admin Password and HTTP Admin Port must not be specified.
HTTP SSL Port	443	The port on which the Web server will listen for SSL requests. Typically, this is set to 443. If the Web server instance is run as non-root this value has to be greater than 1024.
IHS System Group	webadmin	The group that owns and runs the Web server instances and the plug-in directories. If the system group account does not already exist the account will be created on the target machine.
IHS System Password	SysPsWd	The password for the user that owns and runs the Web server instances and the plug-in directories. This password will be used when creating the system user.
IHS System User	ihsadmin	The user that owns and runs the Web server instances and the plug-in directories. If the system user account does not already exist the account will be created on the target machine.
SSL Key Database Password	SslKeyDbPsWd	The password that will be used to create the SSL key database used to store the Web server instance SSL certificates.

Note: For this use case you need to expose the following parameters in the Gather Advanced Parameters for Provision IBM HTTP Server step:

- The IHS System parameters: IHS System Group, IHS System Password, and IHS System User
- The HTTP Admin parameters: HTTP Admin Password, HTTP Admin Port, and HTTP Admin User
- The SSL parameters: HTTP SSL Port and SSL Key Database Password

Parameters for WebSphere - Provision IBM HTTP Server

The following tables describe the required and optional input parameters for this workflow. Most of these parameters are not initially visible in a deployment. For many parameters, if you do not specify a value for a parameter, a default value is assigned

Input Parameters Defined in this Step: Gather Parameters for Provision IBM HTTP Server

Parameter Name	Default Value	Required	Description
Http Port	80	required	The port on which the Web server will listen. Default is set to 80. If the Web server instance is run as non-root this value has to be greater than 1024.
IHS Binary Download Location	no default	required	Name of the compressed IHS software package.
IHS Binary Files	no default	required	Name of the compressed IHS software package.
IHS Extract Location	no default	required	Fully-qualified path where the compressed software will be extracted on the target machine. This cannot be the same as the Install Manager Extract Location.
IHS Install Location	no default	required	Fully-qualified path where IHS will be installed.
Install Manager Binary Download Location	no default	required	Fully-qualified path to the compressed Install Manager software package on the target machine.
Install Manager Binary Files	no default	required	Name of the compressed Install Manager software package.
Install Manager Extract Location	no default	required	Fully-qualified path where the compressed software will be extracted on the target machine. This location cannot be the same as the IHS Extract Location.
Install Manager Install Location	no default	required	Fully-qualified path where the Install Manager will be installed.
License Acceptance	false	required	Acknowledges that the end user agrees to the IBM International Program License Agreement. This is set to false by default and must be set to true for the installation to continue.
Web Server Name	no default	required	Required: Fully-qualified name of the Web server instance. There can be no spaces in the name. For example: <code>myapp.hp.com</code>
Windows Password	no default	required	Password for the Windows Administrator.

Input Parameters Defined in this Step: Gather Parameters for Provision IBM HTTP Server, continued

Parameter Name	Default Value	Required	Description
Windows Username	no default	required	Windows Administrator username.

Additional Input Parameters Defined in this Step: Gather Advanced Parameters for Provision IBM HTTP Server

Parameter Name	Default Value	Required	Description
Access Log File	see description	optional	Fully-qualified path for the IBM HTTP Server access log file. For example: /opt/IBM/HTTPServer/logs The default is based on the values of IHS Install Location and Web Server Name.
Call Wrapper	no default	required	The jython call wrapper required to run as the owner of the files/directories.
Cleanup on Failure	True	optional	Indicates whether to remove downloaded and extracted files and to clean up the installation directory in the event of workflow failure. Valid values are True and False. The default is True, which will clean up on failure.
Cleanup on Success	True	optional	Indicates whether to remove downloaded and extracted files and to clean up the installation directory in the event of workflow success. Valid values are True and False. The default is True, which will clean up on success.
Error Log File	see description	optional	Fully-qualified path for the IBM HTTP Server error log file. For example: /opt/IBM/HTTPServer/logs The default is based on the values of IHS Install Location and Web Server Name.
HTTP Admin Password	no default	optional	Password for the HTTP Admin User. If specified, HTTP Admin Port and HTTP Admin User must also be specified. If not specified, HTTP Admin Port and HTTP Admin User must not be specified.
HTTP Admin Port	no default	optional	Port of the IBM HTTP Server administrative server. If specified, HTTP Admin Password and HTTP Admin User must also be specified. If not specified, HTTP Admin Password and HTTP Admin User must not be specified.
HTTP Admin User	no default	optional	User name of the IBM HTTP administrative user. If specified, HTTP Admin Password and HTTP Admin Port must also be specified. If not specified, HTTP Admin Password and HTTP Admin Port must not be specified.

Additional Input Parameters Defined in this Step: Gather Advanced Parameters for Provision IBM HTTP Server, continued

Parameter Name	Default Value	Required	Description
HTTP Configuration File	see description	optional	Fully-qualified path for the IBM HTTP Server configuration file. For example: /opt/IBM/HTTPServer/conf/httpd.conf The default is based on the values of IHS Install Location and Web Server Name.
HTTP SSL Port	no default	optional	The port on which the Web server will listen for SSL requests. Typically, this is set to 443. If the Web server instance is run as non-root this value has to be greater than 1024.
IHS Install Location	no default	required	Full-qualified path
IHS System Group	no default	optional	The group that owns and runs the Web server instances and the plug-in directories. If the system group account does not already exist the account will be created on the target machine.
IHS System Password	no default	optional	The password for the user that owns and runs the Web server instances and the plug-in directories. This password will be used when creating the system user.
IHS System User	no default	optional	The user that owns and runs the Web server instances and the plug-in directories. If the system user account does not already exist the account will be created on the target machine.
IPAddr	see description	optional	IP address that binds the Web server to a specific IP address and ports. The default value is the IP address of \${Server.Name}.
Plugin Install Root	see description	optional	Fully-qualified path where the WebSphere plug-in is installed. The default is based on IHS Install Location.
Response File	see description	optional	Fully-qualified path where the response file that this workflow creates will be located. This file is used to drive the installation. The default is /tmp/installrespFile.xml
SSL Key Database Password	no default	optional	The password that will be used to create the SSL key database used to store the Web server instance SSL certificates.

Provision WebSphere 7 and Custom Node

Use this workflow to install the WebSphere 7 Base core binaries and, optionally, create a custom profile.

A custom profile initially contains an empty node with no servers. The workflow can add (federate) the server to the pertinent cell when the profile is created, or you can add it later yourself.

To use this workflow in your environment, see the following information:

Topic	Information Included
"Prerequisites for this Workflow"	List of prerequisites that must be satisfied before you can run this workflow
"How this Workflow Works"	Information about what the workflow does, including validation checks performed, steps executed, and a high-level process flow
"How to Run this Workflow"	Instructions for running this workflow in your environment
"Sample Scenario"	Examples of typical parameter values for this workflow
Parameters	List of input parameters for this workflow

Prerequisites for this Workflow

Be sure that the following prerequisites are satisfied before you run the Provision WebSphere 7 and Custom Node workflow:

1. This workflow requires unchallenged `sudo` access to a user (typically `root`) who can access all required files and directories.
2. Per the WebSphere 7 documentation, the following system libraries are required before provisioning IBM WebSphere Application Server version 7 on 64-bit Red Hat Linux:

Platform	Required Library
64-bit Red Hat Enterprise Linux version 5	compat-libstdc++-33-3.2.3-61 compat-db-4.2.52-5.1 libXp-1.0.0-8 compat-libstdc++-296-2.96-138 rpm-build-4.4.2-37.el5

Make sure that these libraries exist on each target server before running this workflow. If newer versions of these libraries are available, you can install the newer versions.

3. This workflow will install WebSphere Application Server as `root` because of the following IBM documented limitations:
 - Creation of a Linux service for WebSphere Application Server
 - Native registration with the operating system
 - Port conflicts that may occur with other installations of WebSphere Application Server that are not registered with the operating system

If there is a need to run as a non-root user after installation, you can run a recursive `chown` under the installation root and set owner permissions accordingly.

For more information about prerequisites for WebSphere 7, refer to the [WebSphere 8 Product Documentation](#).

How this Workflow Works

This topic contains the following information about the Provision WebSphere 7 and Custom Node workflow:

Overview

This workflow does the following things in the order shown:

1. Prepares and validates all parameters and creates the call wrapper that will be used to execute commands within a WebSphere 7 environment
2. Checks the documented library requirements, files system space requirements, and temporary space requirements
3. Checks whether the WebSphere 7 binaries are available—if not, they will be downloaded from the software repository—and extracts the binary files from the compressed archive
4. Creates a new response file
5. Provisions IBM WebSphere Application Server version 7 on a target machine
6. Creates a custom node profile
7. Optionally federates the custom managed node profile into a Deployment Manager

Validation Checks Performed

Most of the validation centers on special characters and spaces in the parameters. There are also validation checks that happen at the operating system level, including file system space checks and RPM checks for Red Hat Linux.

The workflow first performs the following parameter checks:

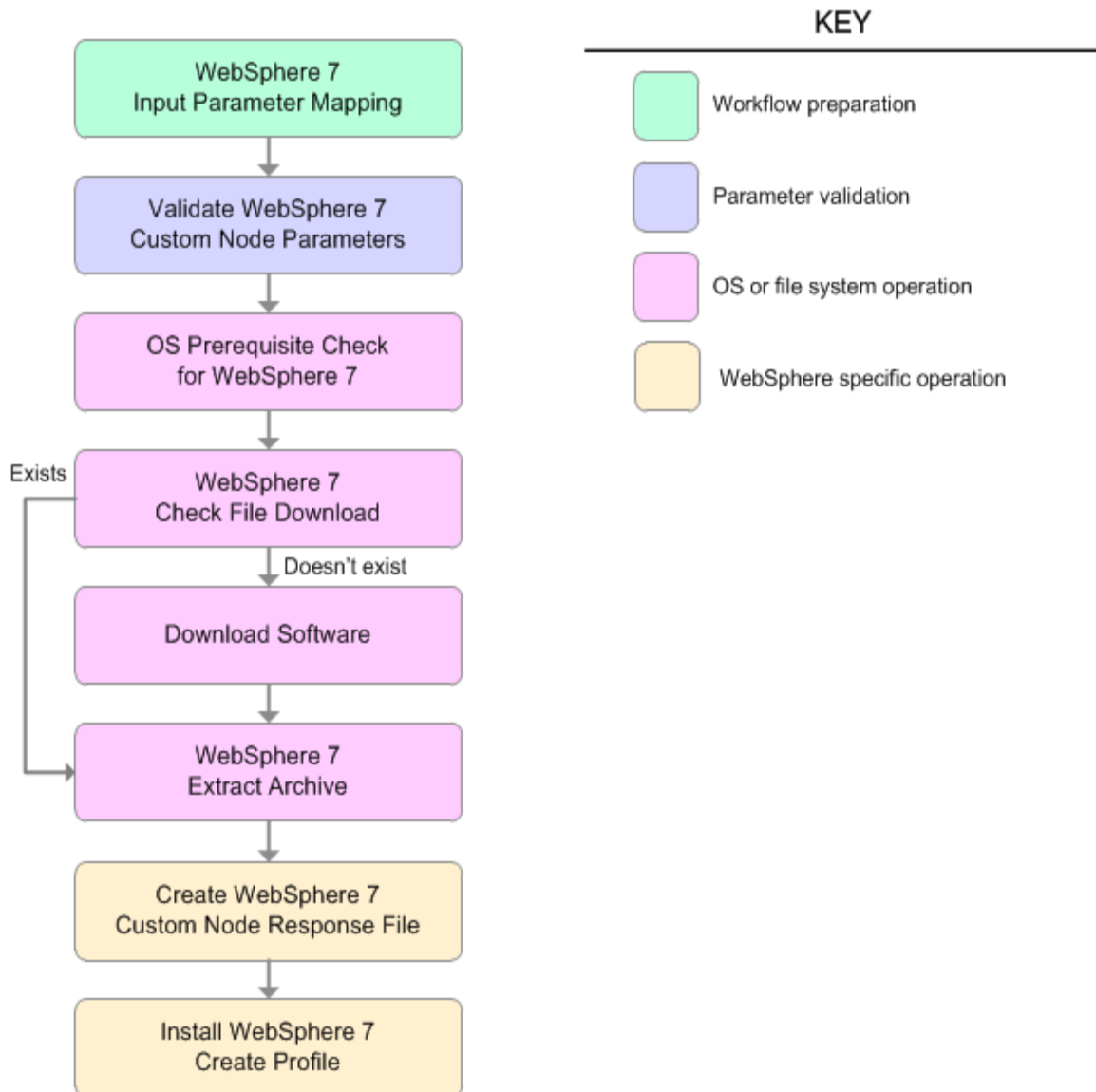
1. Enable Security is true or false. If Enable Security is true, Admin Password and Admin User are specified.
2. Admin User (if specified) does not begin with a period (.), hyphen (-) or space. It does not contain any of the following characters: / \ * , ; = + ? | < > & % ' " [] # \$ ^ { }
3. Admin Password (if specified) does not begin with a hyphen (-) or contain a space.
4. Cell Name, Node Name, and Profile Name are specified. They do not contain the following characters: / \ * , ; = + ? | < > & % ' " [] # \$ ^ { } or space. They do not begin with a period.
5. Host Name is specified.
6. Ports File (if specified) exists.
7. Federate Later (if specified) is true or false.
8. Dmgr HostName is specified.
9. Dmgr Port (if specified) is an integer.
10. License Acceptance is true.
11. Binary Archive is specified. It either exists or can be created successfully.
12. Extract Path and Install Location either exist or can be created successfully.
13. Profile Path and Response File are specified.
14. Profile Type is custom.

The workflow then performs the following operating system checks on the target machine:

1. All required libraries are present (see ["Prerequisites for this Workflow" on page 1210](#)).
2. Sufficient disk space is available to install WebSphere 7.
3. Sufficient disk space is available to extract the binary files from the compressed archive.

Steps Executed

The Provision WebSphere 7 and Custom Node workflow includes the following steps. Each step must complete successfully before the next step can start. If a step fails, the workflow reports a failure, and all subsequent steps are skipped.



Steps Used in the Provision WebSphere 7 and Custom Node Workflow

Workflow Step	Description
WebSphere 7 Input Parameter Mapping	This step creates the call wrapper—the command that executes the step as a specific user—and allows certain parameters to be hidden or exposed.
Validate WebSphere 7 Custom Node Parameters	This step prepares and validates the parameters needed to install WebSphere Application Server V7.0 and create a custom node profile.
OS Prerequisite Check for WebSphere 7	This step checks the documented library requirements, files system space requirements, and temporary space requirements for WebSphere Application Server V7.0.
WebSphere 7 Check File Download	<p>This step checks for the existence of a file before downloading it from the software repository:</p> <ul style="list-style-type: none"> • Checks if a file exists in the expected location. • If the file is not in the expected location, the file is added to a list of files that need to be downloaded.

Steps Used in the Provision WebSphere 7 and Custom Node Workflow, continued

Workflow Step	Description
Download Software	This step downloads a list of files to a specified location on the target server.
WebSphere 7 Extract Archive	This step checks that the archive file exists and then, based on the archive extension, extracts the archive to the specified directory.
Create WebSphere 7 Custom Node Response File	This step creates a new response file for installing a new instance of WebSphere Application Server V7.0 and creating a custom node profile.
Install WebSphere 7 Create Profile	This step installs a new instance of WebSphere Application Server V7.0 using the <code>install -options <responsefile> silent</code> option and then creates a profile.

For parameter descriptions and defaults, see ["Parameters for Provision WebSphere 7 and Custom Node" on page 1222](#).

How to Run this Workflow

The following instructions show you how to customize and run the Provision WebSphere 7 and Custom Node workflow in your environment.

The workflow provides default values for some parameters. These default values are usually sufficient for a "typical" installation. You can override the defaults by specifying parameter values in the deployment. You can also expose additional parameters in the workflow, if necessary, to accomplish more advanced scenarios. Any parameters not explicitly specified in the deployment will have the default values listed in ["Parameters for Provision WebSphere 7 and Custom Node" on page 1222](#).

Note: Before following this procedure, review the ["Prerequisites for this Workflow"](#), and ensure that all requirements are satisfied.

To customize and run the Provision WebSphere 7 and Custom Node workflow:

1. Create a deployable copy of the workflow.
2. Determine the values that you will specify for the following parameters:

Input Parameters for Validate WebSphere 7 Custom Node Parameters

Parameter Name	Default Value	Required	Description
Binary Archive	no default	required	Fully qualified path to the compressed software package on the target machine. For example: /opt/install/C1G36ML.tar.gz
Cell Name	no default	required	Unique cell name that does not contain any of the following special characters / \ * , ; : = + ? < > & % ' " [] # \$ ^ { }. If you plan to federate into an existing cell later, make sure that this name is not the same as the existing cell name.
Dmgr Admin Password	no default	optional	Administrative user password for the Deployment Manager. When Enable Security is set to true, this parameter must contain a string that does not begin with a dash(-) or contain a space().
Dmgr Admin User	no default	optional	Deployment Manager administrative user. When Enable Security is set to true, this parameter must contain a string that does not begin with a dash(-), a period(.), or a space(). It cannot contain any of the following characters / \ * , ; : = + ? < > & % ' " [] # \$ ^ { }.
Dmgr HostName	no default	optional	Host name or IP address of the machine where the Deployment Manager is running. Specify this parameter and the Dmgr Port parameter to federate the new custom node as it is created. If you do not specify a value for this parameter, the new custom node is not federated (you

Input Parameters for Validate WebSphere 7 Custom Node Parameters, continued

Parameter Name	Default Value	Required	Description
			must federate it later). Required if Federate Later is set to false.
Dmgr Port	no default	optional	The SOAP port on which the Deployment Manager is listening. Specify this parameter and the Dmgr Host Name parameter to federate the new custom node as it is created. If you do not specify a value for this parameter, the new custom node is not federated (you must federate it later). Required if Federate Later is set to false.
Enable Security	no default	required	Enables administrative security on the Deployment Manager. Must be set to either true or false. If Enable Security is true, the Dmgr Admin User and Dmgr Admin Password parameters must have values.
Extract Dir	no default	required	Fully qualified path where the compressed software will be extracted on the target machine.
Federate Later	no default	required	If false, the new custom node will be federated by the workflow during profile creation. If true, you must federate it later manually by using the addNode command.
Install Location	no default	required	Fully qualified path where WebSphere Application Server will be installed. For example: /opt/IBM/WebSphere/AppServer
License Acceptance	false	required	Acknowledges that the end user agrees to the IBM International Program License Agreement. This is set to false by default and must be set to true in order for the installation to continue.
Node Name	no default	required	Unique node name that cannot contain any of the following special characters / \ * , ; = + ? < > & % ' " [] # \$ ^ { }. If you plan to federate into an existing cell later, make sure that the name is unique within that cell.
Profile Name	no default	required	A unique profile name. It cannot begin with a period (.) and cannot contain any of the following special characters / \ * , ; = + ? < > & % ' " [] # \$ ^ { }.
Profile Path	no default	required	Fully qualified path to the custom node profile. For example: /opt/IBM/WebSphere/AppServer/ profiles/ProdNode01
Profile Type	custom	required	Because this workflow creates a Custom Node profile, the value must be custom.
Response File	no default	required	Fully qualified path where the response file that this workflow creates will be located. This file will then be used to drive the installation and profile creation.

Additional Input Parameters for Install WebSphere 7 Create Profile

Parameter Name	Default Value	Required	Description
Password	no default	required	The Windows Administrator password. Required for Windows.
Username	no default	required	This is the Windows Administrator user. Required for Windows.

Note: This is the minimum set of parameters required to run this workflow. You may need to expose additional parameters depending on your provisioning objectives.

See ["Parameters for Provision WebSphere 7 and Custom Node" on page 1222](#) for detailed descriptions of all input parameters for this workflow, including default values.

Tip: To avoid having to re-enter passwords whenever they change, you can create a policy to provide them to the workflow.

3. In the workflow editor, expose any additional parameters that you need. You will specify values for those parameters when you create the deployment.
4. Save the changes to the workflow (click **Save** in the lower right corner).
5. Create a new deployment.
6. On the Parameters tab, specify values for the required parameters listed in step 2 and any additional parameters that you have exposed. You do not need to specify values for those parameters whose default values are appropriate for your environment.
7. On the Targets tab, specify one or more targets for this deployment.
8. Save the deployment (click **Save** in the lower right corner).
9. Run the workflow using this deployment.

To verify the results:

Optional: if you want to further verify the results, perform the following steps:

1. After the workflow has completed, run the following command to check the version of WebSphere Application Server that was installed:

```
WAS_ROOT/bin/versionInfo.sh
```

Here, *WAS_ROOT* is the directory where WebSphere 7 is installed. This is the path that you specified in the WebSphere Install Location parameter.

2. Validate that the Deployment Manager profile has been created and is running by doing the following:
 - a. View the *WAS_ROOT/profiles/PROFILE_NAME/logs/AboutThisProfile.txt* file. This file is created after the creation of the profile and contains specific information about the profile.

Here, *PROFILE_NAME* is the name of the profile that you just created. This is the name that you specified in the Profile Name parameter.

- b. Change to the *WAS_ROOT/profiles/PROFILE_NAME/logs/nodeagent* directory, and tail the *SystemOut.log* file. Look for the following line:

```
Server nodeagent open for e-business
```

Sample Scenario

This topic shows you typical parameter values used for the Provision WebSphere 7 and Custom Node workflow.

New WebSphere 7 install with custom node profile

Input Parameters for Validate WebSphere 7 Custom Node Parameters

Parameter Name	Example Value	Description
Binary Archive	see description	Fully qualified path to the compressed software package on the target machine. For example: /opt/install/C1G36ML.tar.gz
Cell Name	Dev NodeCell	Unique cell name that does not contain any of the following special characters / \ * , ; = + ? < > & % ' " [] # \$ ^ { }. If you plan to federate into an existing cell later, make sure that this name is not the same as the existing cell name.
Dmgr Admin Password	wasPassWord	Administrative user password for the Deployment Manager. When Enable Security is set to true, this parameter must contain a string that does not begin with a dash(-) or contain a space().
Dmgr Admin User	wasadmin	Deployment Manager administrative user. When Enable Security is set to true, this parameter must contain a string that does not begin with a dash(-), a period(.), or a space(.). It cannot contain any of the following characters / \ * , ; = + ? < > & % ' " [] # \$ ^ { }.
Dmgr HostName	mycompany.com	Host name or IP address of the machine where the Deployment Manager is running. Specify this parameter and the Dmgr Port parameter to federate the new custom node as it is created. If you do not specify a value for this parameter, the new custom node is not federated (you must federate it later). Required if Federate Later is set to false.
Dmgr Port	8879	The SOAP port on which the Deployment Manager is listening. Specify this parameter and the Dmgr Host Name parameter to federate the new custom node as it is created. If you do not specify a value for this parameter, the new custom node is not federated (you must federate it later). Required if Federate Later is set to false.
Enable Security	true	Enables administrative security on the Deployment Manager. Must be set to either true or false. If Enable Security is true, the Dmgr Admin User and Dmgr Admin Password parameters must have values.
Extract Dir	/opt/IBM/wasv7	Fully qualified path where the compressed software will be extracted on the target machine.
Federate Later	true	If false, the new custom node will be federated by the workflow during profile creation; you must specify Dmgr HostName and Dmgr Port to do this. If true, you must federate it later manually by using the addNode command.
Install	see description	Fully qualified path where WebSphere Application Server will be

Input Parameters for Validate WebSphere 7 Custom Node Parameters, continued

Parameter Name	Example Value	Description
Location		installed. For example: /opt/IBM/WebSphere/AppServer
License Acceptance	true	Acknowledges that the end user agrees to the IBM International Program License Agreement. This is set to false by default and must be set to true in order for the installation to continue.
Node Name	DevNode	Unique node name that cannot contain any of the following special characters / \ * , ; = + ? < > & % ' " [] # \$ ^ { }. If you plan to federate into an existing cell later, make sure that the name is unique within that cell.
Profile Name	DevNode	A unique profile name. It cannot begin with a period (.) and cannot contain any of the following special characters / \ * , ; = + ? < > & % ' " [] # \$ ^ { }.
Profile Path	see description	Fully qualified path to the custom node profile. For example: /opt/IBM/WebSphere/AppServer/ profiles/ProdNode01
Profile Type	custom	Because this workflow creates a Custom Node profile, the value must be custom.
Response File	/tmp/serverrsp	Fully qualified path where the response file that this workflow creates will be located. This file will then be used to drive the installation and profile creation.

Tip: To avoid having to re-enter passwords whenever they change, you can create a policy to provide them to the workflow.

Parameters for Provision WebSphere 7 and Custom Node

Tip: To avoid having to re-enter passwords whenever they change, you can create a policy to provide them to the workflow.

Note: Only those parameters that are configurable in a standard deployment are listed here. Input parameters that must be mapped to output parameters of previous steps are not listed.

Parameters Defined in this Step: Validate WebSphere 7 Custom Node Parameters

Parameter Name	Default Value	Required	Description
Binary Archive	no default	required	Fully qualified path to the compressed software package on the target machine. For example: <code>/opt/install/C1G36ML.tar.gz</code>
Call Wrapper	see description	required	Command that will execute this step (or subsequent steps) as a specific user. For UNIX targets, the default is: <code>/opt/hp/dma/client/jython.sh</code> running as root For Windows targets, the default is: <code>jython</code> running as Administrator <div>This parameter is derived by the workflow. Under most circumstances, you should not change its mapping or its value.</div>
Cell Name	no default	required	Unique cell name that does not contain any of the following special characters <code>/ \ * , ; = + ? < > & % ' " [] # \$ ^ { }</code> . If you plan to federate into an existing cell later, make sure that this name is not the same as the existing cell name.
Dmgr Admin Password	no default	optional	Administrative user password for the Deployment Manager. When Enable Security is set to true, this parameter must contain a string that does not begin with a dash(-) or contain a space().
Dmgr Admin User	no default	optional	Deployment Manager administrative user. When Enable Security is set to true, this parameter must contain a string that does not begin with a dash(-), a period(.), or a space(). It cannot contain any of the following characters <code>/ \ * , ; = + ? < > & % ' " [] # \$ ^ { }</code> .
Dmgr HostName	no default	optional	Host name or IP address of the machine where the Deployment Manager is running. Specify this parameter and the Dmgr Port parameter to federate the new custom node as it is created. If you do not specify a value for this parameter, the new custom node is not federated (you must federate it later). Required if Federate Later is set to false.

Parameters Defined in this Step: Validate WebSphere 7 Custom Node Parameters, continued

Parameter Name	Default Value	Required	Description
Dmgr Port	no default	optional	The SOAP port on which the Deployment Manager is listening. Specify this parameter and the Dmgr Host Name parameter to federate the new custom node as it is created. If you do not specify a value for this parameter, the new custom node is not federated (you must federate it later). Required if Federate Later is set to false.
Enable Security	no default	required	Enables administrative security on the Deployment Manager. Must be set to either true or false. If Enable Security is true, the Dmgr Admin User and Dmgr Admin Password parameters must have values.
Extract Dir	no default	required	Fully qualified path where the compressed software will be extracted on the target machine.
Federate Later	no default	required	If false, the new custom node will be federated by the workflow during profile creation. If true, you must federate it later manually by using the addNode command.
Host Name	Server.name	required	Hostname or IP address of the target machine.
Install Location	no default	required	Fully qualified path where WebSphere Application Server will be installed. For example: /opt/IBM/WebSphere/AppServer
Keystore Password	no default	required	Sets the password for all keystore files created during profile creation. This includes keystore files for both the default personal certificate and the root signing certificate.
License Acceptance	false	required	Acknowledges that the end user agrees to the IBM International Program License Agreement. This is set to false by default and must be set to true in order for the installation to continue.
Node Name	no default	required	Unique node name that cannot contain any of the following special characters / \ * , ; = + ? < > & % ' " [] # \$ ^ { }. If you plan to federate into an existing cell later, make sure that the name is unique within that cell.
Personal CertDN	no default	optional	Distinguished name of the personal certificate. For example: CN=dmlab-example.com,OU=WAS7LabCell,OU=WAS7LabDmgrManager,O=IBM,C=US The DN string cannot contain spaces. If you do not specify the DN, the WebSphere Application Server installer will create one.
Personal CertValidity Period	1	optional	Amount of time in years that the personal certificate is valid. Default is one year.

Parameters Defined in this Step: Validate WebSphere 7 Custom Node Parameters, continued

Parameter Name	Default Value	Required	Description
Ports File	no default	optional	Fully qualified path to a file that defines port settings for the new profile. This file must contain key=value pairs that specify a service name and a port number (for example: WC_adminhost=9060). This option should be used with the Validate Ports option.
Profile Name	no default	required	A unique profile name. It cannot begin with a period (.) and cannot contain any of the following special characters <code>/ \ * , : ; = + ? < > & % ' " [] # \$ ^ { }</code> .
Profile Path	no default	required	Fully qualified path to the custom node profile. For example: <code>/opt/IBM/WebSphere/AppServer/ profiles/ProdNode01</code>
Profile Type	no default	required	Because this workflow creates a Custom Node profile, the value must be custom.
Response File	no default	required	Fully qualified path where the response file that this workflow creates will be located. This file will then be used to drive the installation and profile creation.
Signing CertDN	no default	optional	Distinguished name of the signing certificate. For example: <code>CN=dmlab-example.com, OU=Root Certificate, OU=WAS7TestLabCell, OU=WAS7LabNode1, O=IBM, C=US</code> The DN string cannot contain spaces. If you do not specify the DN, the WebSphere Application Server installer will create one.
Signing CertValidity Period	15	optional	Amount of time in years that the root certificate is valid. Default is 15 years.

Additional Parameters Defined in this Step: Install WebSphere 7 Create Profile

Parameter Name	Default Value	Required	Description
Password	no default	required	The Windows Administrator password. Required for Windows.
Username	no default	required	This is the Windows Administrator user. Required for Windows.

Provision WebSphere 7 and Deployment Manager

Use this workflow to install the WebSphere 7 Base core binaries and, optionally, create a Deployment Manager profile.

A Deployment Manager is the administration point for a cell that contains multiple application servers. This type of profile is appropriate for distributed application server environments.

To use this workflow in your environment, see the following information:

Topic	Information Included
"Prerequisites for this Workflow"	List of prerequisites that must be satisfied before you can run this workflow
"How this Workflow Works"	Information about what the workflow does, including validation checks performed, steps executed, and a high-level process flow
"How to Run this Workflow"	Instructions for running this workflow in your environment
"Sample Scenario"	Examples of typical parameter values for this workflow
Parameters	List of input parameters for this workflow

Prerequisites for this Workflow

Be sure that the following prerequisites are satisfied before you run the Provision WebSphere 7 and Deployment Manager workflow:

1. This workflow requires unchallenged `sudo` access to a user (typically `root`) who can access all required files and directories.
2. Per the WebSphere 7 documentation, the following system libraries are required before provisioning IBM WebSphere Application Server version 7 on 64-bit Red Hat Linux:

Platform	Required Library
64-bit Red Hat Enterprise Linux version 5	compat-libstdc++-33-3.2.3-61 compat-db-4.2.52-5.1 libXp-1.0.0-8 compat-libstdc++-296-2.96-138 rpm-build-4.4.2-37.el5

Make sure that these libraries exist on each target server before running this workflow. If newer versions of these libraries are available, you can install the newer versions.

3. This workflow will install WebSphere Application Server as `root` because of the following IBM documented limitations:
 - Creation of a Linux service for WebSphere Application Server
 - Native registration with the operating system
 - Port conflicts that may occur with other installations of WebSphere Application Server that are not registered with the operating system

If there is a need to run as a non-root user after installation, you can run a recursive `chown` under the installation root and set owner permissions accordingly.

For more information about prerequisites for WebSphere 7, refer to the [WebSphere 8 Product Documentation](#).

How this Workflow Works

This topic contains the following information about the Provision WebSphere 7 and Deployment Manager workflow:

Overview

This workflow does the following things in the order shown:

1. Prepares and validates all parameters and creates the call wrapper that will be used to execute commands within a WebSphere 7 environment
2. Checks the documented library requirements, files system space requirements, and temporary space requirements
3. Checks whether the WebSphere 7 binaries are available—if not, they will be downloaded from the software repository—and extracts the binary files from the compressed archive
4. Creates a new response file
5. Provisions IBM WebSphere Application Server version 7 on a target machine
6. Creates a Deployment Manager profile
7. Starts the WebSphere 7 Deployment Manager application server

Validation Checks Performed

Most of the validation centers on special characters and spaces in the parameters. There are also validation checks that happen at the operating system level, including file system space checks and RPM checks for Red Hat Linux.

The workflow first performs the following parameter checks:

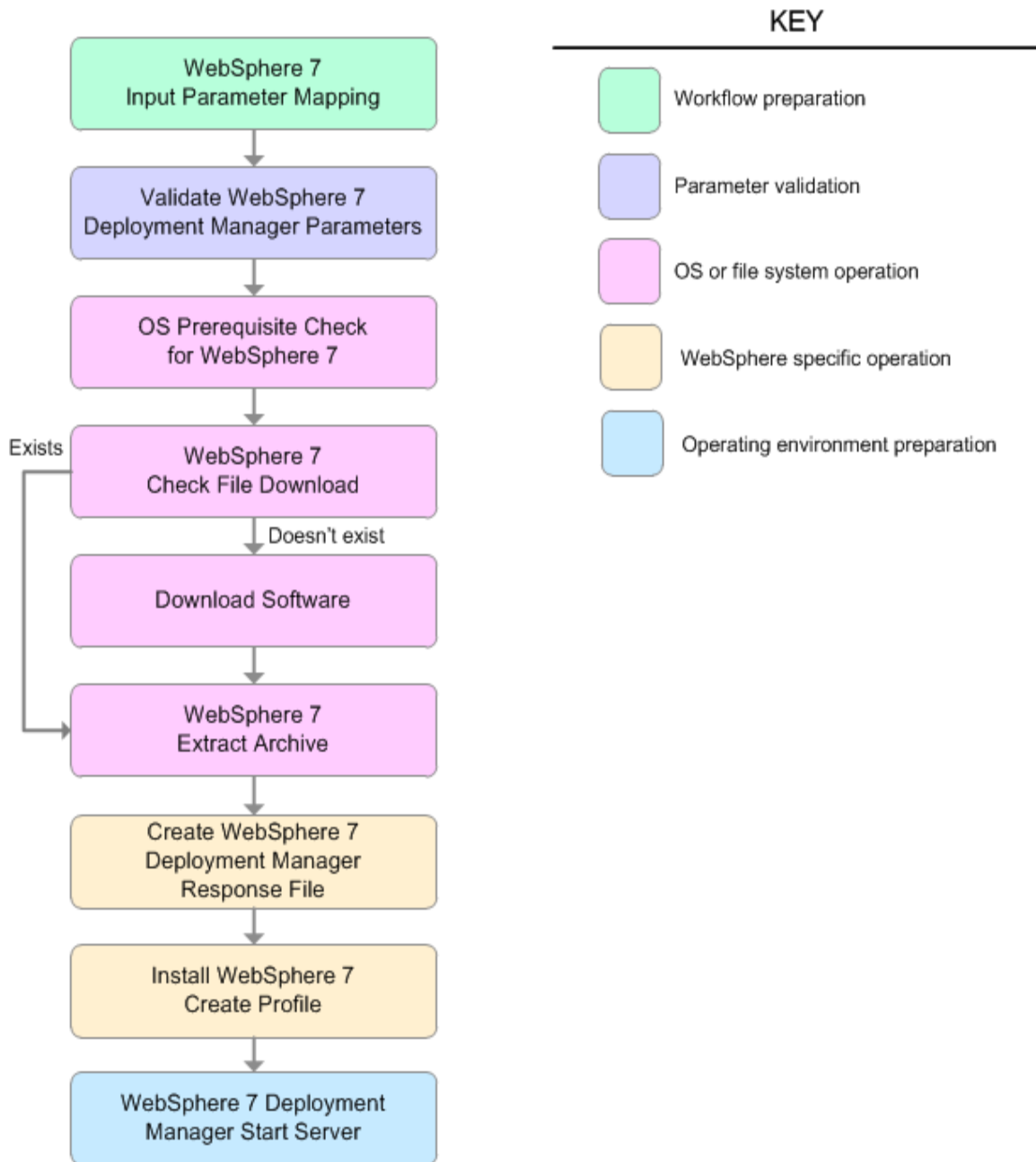
1. Admin User (if specified) does not begin with a period (.), hyphen (-) or space. It does not contain any of the following characters: / \ * , ; = + ? | < > & % ' " [] # \$ ^ { }
2. Admin Password (if specified) does not begin with a hyphen (-) or contain a space.
3. Cell Name, Node Name, and Profile Name are specified. They do not contain the following characters: / \ * , ; = + ? | < > & % ' " [] # \$ ^ { } or space. They do not begin with a period.
4. Host Name is specified.
5. Default Ports (if specified) is true or false.
6. Enable Security is true or false. If Enable Security is true, Admin Password and Admin User are specified.
7. Omit Action (if specified) is defaultAppDeployAndConfig, or deployAdminConsole.
8. Ports File (if specified) exists and Validate Ports is true or false.
9. Starting Port (if specified) is an integer.
10. If the operating system is Windows, Windows Admin User and Windows Admin Password are specified.
11. License Acceptance is true.
12. Binary Archive is specified. It either exists or can be created successfully.
13. Extract Path and Install Location either exist or can be created successfully.
14. Profile Path and Response File are specified.
15. Server Type is DEPLOYMENT_MANAGER.
16. Profile Type is management.

The workflow then performs the following operating system checks on the target machine:

1. All required libraries are present (see ["Prerequisites for this Workflow" on page 1226](#)).
2. Sufficient disk space is available to install WebSphere 7.
3. Sufficient disk space is available to extract the binary files from the compressed archive.

Steps Executed

The Provision WebSphere 7 and Deployment Manager workflow includes the following steps. Each step must complete successfully before the next step can start. If a step fails, the workflow reports a failure, and all subsequent steps are skipped.



Steps Used in the Provision WebSphere 7 and Deployment Manager Workflow

Workflow Step	Description
WebSphere 7 Input Parameter Mapping	This step creates the call wrapper—the command that executes the step as a specific user—and allows certain parameters to be hidden or exposed.
Validate WebSphere 7 Deployment Manager Parameters	This step prepares and validates the parameters needed to install WebSphere Application Server V7.0 and create a Deployment Manager profile.
OS Prerequisite Check for WebSphere 7	This step checks the documented library requirements, files system space requirements, and temporary space requirements for WebSphere Application Server V7.0.
WebSphere 7 Check File Download	<p>This step checks for the existence of a file before downloading it from the software repository:</p> <ul style="list-style-type: none"> • Checks if a file exists in the expected location. • If the file is not in the expected location, the file is added to a list of files that need to be downloaded.
Download Software	This step downloads a list of files to a specified location on the target server.
WebSphere 7 Extract Archive	This step checks that the archive file exists and then, based on the archive extension, extracts the archive to the specified directory.
Create WebSphere 7 Deployment Manager Response File	This step creates a new response file for installing a new instance of WebSphere Application Server V7.0 and creating a Deployment Manager profile.
Install WebSphere 7 Create Profile	This step installs a new instance of WebSphere Application Server V7.0 using the <code>install -options</code>

Steps Used in the Provision WebSphere 7 and Deployment Manager Workflow, continued

Workflow Step	Description
	<responsefile> silent option and then creates a profile.
WebSphere 7 Deployment Manager Start Server	This step starts the WebSphere 7 Deployment Manager application server.

For parameter descriptions and defaults, see ["Parameters for Provision WebSphere 7 and Deployment Manager" on page 1238](#).

How to Run this Workflow

The following instructions show you how to customize and run the Provision WebSphere 7 and Deployment Manager workflow in your environment.

The workflow provides default values for some parameters. These default values are usually sufficient for a "typical" installation. You can override the defaults by specifying parameter values in the deployment. You can also expose additional parameters in the workflow, if necessary, to accomplish more advanced scenarios. Any parameters not explicitly specified in the deployment will have the default values listed in ["Parameters for Provision WebSphere 7 and Deployment Manager" on page 1238](#).

Note: Before following this procedure, review the ["Prerequisites for this Workflow"](#), and ensure that all requirements are satisfied.

To customize and run the Provision WebSphere 7 and Deployment Manager workflow:

1. Create a deployable copy of the workflow.
2. Determine the values that you will specify for the following parameters:

Input Parameters for Validate WebSphere 7 Deployment Manager Parameters

Parameter Name	Default Value	Required	Description
Admin Password	no default	optional	When Enable Security is set to true, this parameter must contain a string that does not begin with a dash(-) or contain a space().
Admin User	no default	optional	When Enable Security is set to true, this parameter must contain a string that does not begin with a dash(-), a period(.), or a space(). It cannot contain any of the following characters / \ * , ; = + ? < > & % ' " [] # \$ ^ { }.
Binary Archive	no default	required	Fully qualified path to the compressed software package on the target machine. For example: /opt/install/C1G36ML.tar.gz
Cell Name	no default	required	Unique cell name that does not contain any of the following special characters / \ * , ; = + ? < > & % ' " [] # \$ ^ { }. If you plan to federate into an existing cell later, make sure that this name is not the same as the existing cell name.
Enable Security	no default	required	Enables administrative security. Must be set to either true or false. If Enable Security is true, the Admin User and Admin Password parameters must have values.

Input Parameters for Validate WebSphere 7 Deployment Manager Parameters, continued

Parameter Name	Default Value	Required	Description
Extract Dir	no default	required	Fully qualified path where the compressed software will be extracted on the target machine.
Install Location	no default	required	Fully qualified path where WebSphere Application Server will be installed. For example: /opt/IBM/WebSphere/AppServer
License Acceptance	false	required	Acknowledges that the end user agrees to the IBM International Program License Agreement. This is set to false by default and must be set to true in order for the installation to continue.
Node Name	no default	required	Unique node name that cannot contain any of the following special characters / \ * , ; = + ? < > & % ' " [] # \$ ^ { }. If you plan to federate into an existing cell later, make sure that the name is unique within that cell.
Profile Name	no default	required	A unique profile name. It cannot begin with a period (.) and cannot contain any of the following special characters / \ * , ; = + ? < > & % ' " [] # \$ ^ { }.
Profile Path	no default	required	Fully qualified path to the Deployment Manager profile. For example: /opt/IBM/WebSphere/AppServer/ profiles/ProdDmgr
Profile Type	management	required	Because this workflow creates a Deployment Manager profile, the value must be management.
Response File	no default	required	Fully qualified path where the response file that this workflow creates will be located. This file will then be used to drive the installation and profile creation.
Server Type	DEPLOYMENT_MANAGER	required	The type of management profile. The value is DEPLOYMENT_MANAGER for a deployment manager server.
Windows Admin Password	no default	required	The Windows Administrator password. Required for Windows.
Windows Admin User	no default	required	This is the Windows Administrator user. Required for Windows.

Note: This is the minimum set of parameters required to run this workflow. You may need to expose additional parameters depending on your provisioning objectives.

See ["Parameters for Provision WebSphere 7 and Deployment Manager" on page 1238](#) for detailed descriptions of all input parameters for this workflow, including default values.

Tip: To avoid having to re-enter passwords whenever they change, you can create a policy to provide them to the workflow.

3. In the workflow editor, expose any additional parameters that you need. You will specify values for those parameters when you create the deployment.
4. Save the changes to the workflow (click **Save** in the lower right corner).
5. Create a new deployment.
6. On the Parameters tab, specify values for the required parameters listed in step 2 and any additional parameters that you have exposed. You do not need to specify values for those parameters whose default values are appropriate for your environment.
7. On the Targets tab, specify one or more targets for this deployment.
8. Save the deployment (click **Save** in the lower right corner).
9. Run the workflow using this deployment.

To verify the results:

The workflow will complete and report SUCCESS on the Console if it has run successfully. If an error occurs during workflow execution, the error is logged, and the workflow terminates in the FAILURE state.

Optional: if you want to further verify the results, perform the following steps:

1. After the workflow has completed, run the following command to check the version of WebSphere Application Server that was installed:

```
WAS_ROOT/bin/versionInfo.sh
```

Here, *WAS_ROOT* is the directory where WebSphere 7 is installed. This is the path that you specified in the WebSphere Install Location parameter.

2. Validate that the Deployment Manager profile has been created and is running by doing the following:
 - a. View the *WAS_ROOT*/profiles/*PROFILE_NAME*/logs/AboutThisProfile.txt file. This file is created after the creation of the profile and contains specific information about the profile.

Here, *PROFILE_NAME* is the name of the profile that you just created. This is the name that you specified in the Profile Name parameter.

- b. Change to the *WAS_ROOT*/profiles/*PROFILE_NAME*/logs/dmgr directory, and tail the SystemOut.log file. Look for the following line:

```
Server dmgr open for e-business
```

Sample Scenario

This topic shows you typical parameter values used for the Provision WebSphere 7 and Deployment Manager workflow.

New WebSphere 7 install with Deployment Manager profile

Input Parameters for Validate WebSphere 7 Deployment Manager Parameters

Parameter Name	Example Value	Description
Admin Password	wasPassWord	When Enable Security is set to true, this parameter must contain a string that does not begin with a dash(-) or contain a space().
Admin User	wasadmin	When Enable Security is set to true, this parameter must contain a string that does not begin with a dash(-), a period(.), or a space(). It cannot contain any of the following characters / \ * , ; = + ? < > & % ' " [] # \$ ^ { }.
Binary Archive	see description	Fully qualified path to the compressed software package on the target machine. For example: /opt/install/C1G36ML.tar.gz
Cell Name	DevCell	Unique cell name that does not contain any of the following special characters / \ * , ; = + ? < > & % ' " [] # \$ ^ { }. If you plan to federate into an existing cell later, make sure that this name is not the same as the existing cell name.
Enable Security	true	Enables administrative security. Must be set to either true or false. If Enable Security is true, the Admin User and Admin Password parameters must have values.
Extract Dir	/opt/IBM/wasv7	Fully qualified path where the compressed software will be extracted on the target machine.
Install Location	see description	Fully qualified path where WebSphere Application Server will be installed. For example: /opt/IBM/WebSphere/AppServer
License Acceptance	true	Acknowledges that the end user agrees to the IBM International Program License Agreement. This is set to false by default and must be set to true in order for the installation to continue.
Node Name	no default	Unique node name that cannot contain any of the following special characters / \ * , ; = + ? < > & % ' " [] # \$ ^ { }. If you plan to federate into an existing cell later, make sure that the name is unique within that cell.
Profile Name	no default	A unique profile name. It cannot begin with a period (.) and cannot contain any of the following special characters / \ * , ; = + ? < > & % ' " [] # \$ ^ { }.
Profile Path	no default	Fully qualified path to the Deployment Manager profile. For example: /opt/IBM/WebSphere/AppServer/ profiles/ProdDmgr
Profile Type	management	Because this workflow creates a Deployment Manager profile,

Input Parameters for Validate WebSphere 7 Deployment Manager Parameters, continued

Parameter Name	Example Value	Description
		the value must be management.
Response File	/tmp/serverrsp	Fully qualified path where the response file that this workflow creates will be located. This file will then be used to drive the installation and profile creation.
Server Type	DEPLOYMENT_MANAGER	The type of management profile. The value is DEPLOYMENT_MANAGER for a deployment manager server.

Tip: To avoid having to re-enter passwords whenever they change, you can create a policy to provide them to the workflow.

Parameters for Provision WebSphere 7 and Deployment Manager

The following tables describe the required and optional input parameters for this workflow. Some of these parameters may not be initially visible in a deployment. For some parameters, if you do not specify a value for a parameter, a default value is assigned.

Note: Only those parameters that are configurable in a standard deployment are listed here. Input parameters that must be mapped to output parameters of previous steps are not listed.

Parameters Defined in this Step: Validate WebSphere 7 Deployment Manager Parameters

Parameter Name	Default Value	Required	Description
Admin Password	no default	optional	When Enable Security is set to true, this parameter must contain a string that does not begin with a dash (-) or contain a space().
Admin User	no default	optional	When Enable Security is set to true, this parameter must contain a string that does not begin with a dash (-), a period(.), or a space(). It cannot contain any of the following characters / \ * , ; = + ? < > & % ' " [] # \$ ^ { }.
Binary Archive	no default	required	Fully qualified path to the compressed software package on the target machine. For example: /opt/install/C1G36ML.tar.gz
Call Wrapper	see description	required	Command that will execute this step (or subsequent steps) as a specific user. For UNIX targets, the default is: /opt/hp/dma/client/jython.sh running as root For Windows targets, the default is: jython running as Administrator This parameter is derived by the workflow. Under most circumstances, you should not change its mapping or its value.
Cell Name	no default	required	Unique cell name that does not contain any of the following special characters / \ * , ; = + ? < > & % ' " [] # \$ ^ { }. If you plan to federate into an existing cell later, make sure that this name is not the same as the existing cell name.
Default Ports	false	optional	Provides the option to assign default ports to a profile. Valid values are true or false. If true, the WebSphere Application Server default ports will be used, and the Ports File and Starting Port parameters should not have values. If false, the workflow will increment the default port until it finds a free port. The default value is false.

Parameters Defined in this Step: Validate WebSphere 7 Deployment Manager Parameters, continued

Parameter Name	Default Value	Required	Description
Enable Security	no default	required	Enables administrative security. Must be set to either true or false. If Enable Security is true, the Admin User and Admin Password parameters must have values.
Extract Dir	no default	required	Fully qualified path where the compressed software will be extracted on the target machine.
Host Name	Server.name	required	Hostname or IP address of the target machine.
Install Location	no default	required	Fully qualified path where WebSphere Application Server will be installed. For example: /opt/IBM/WebSphere/AppServer
Keystore Password	no default	required	Sets the password for all keystore files created during profile creation. This includes keystore files for both the default personal certificate and the root signing certificate.
License Acceptance	false	required	Acknowledges that the end user agrees to the IBM International Program License Agreement. This is set to false by default and must be set to true in order for the installation to continue.
Node Name	no default	required	Unique node name that cannot contain any of the following special characters / \ * , ; = + ? < > & % ' " [] # \$ ^ { }. If you plan to federate into an existing cell later, make sure that the name is unique within that cell.
Omit Action	no default	optional	Enables you to prevent certain optional features from being installed. Valid values are deployAdminConsole or defaultAppDeployAndConfig. You may only specify one of these options.
Personal CertDN	no default	optional	Distinguished name of the personal certificate. For example: CN=dmlab-example.com,OU=WAS7LabCell,OU=WAS7LabDmgrManager,O=IBM,C=US The DN string cannot contain spaces. If you do not specify the DN, the WebSphere Application Server installer will create one.
Personal CertValidity Period	1	optional	Amount of time in years that the personal certificate is valid. Default is one year.
Ports File	no default	optional	Fully qualified path to a file that defines port settings for the new profile. This file must contain key=value pairs that specify a service name and a port number (for example: WC_adminhost=9060). This option should be used with the Validate Ports option.
Profile	no default	required	A unique profile name. It cannot begin with a period (.)

Parameters Defined in this Step: Validate WebSphere 7 Deployment Manager Parameters, continued

Parameter Name	Default Value	Required	Description
Name			and cannot contain any of the following special characters <code>/ \ * , : ; = + ? < > & % ' " [] # \$ ^ { }</code> .
Profile Path	no default	required	Fully qualified path to the Deployment Manager profile. For example: <code>/opt/IBM/WebSphere/AppServer/profiles/ProdDmgr</code>
Profile Type	management	required	Because this workflow creates a Deployment Manager profile, the value must be management.
Response File	no default	required	Fully qualified path where the response file that this workflow creates will be located. This file will then be used to drive the installation and profile creation.
Server Type	DEPLOYMENT_MANAGER	required	The type of management profile. The value is DEPLOYMENT_MANAGER for a deployment manager server.
Signing CertDN	no default	optional	Distinguished name of the signing certificate. For example: <code>CN=dmalab-example.com, OU=Root Certificate, OU=WAS7TestLabCell, OU=WAS7LabNode1, O=IBM, C=US</code> The DN string cannot contain spaces. If you do not specify the DN, the WebSphere Application Server installer will create one.
Signing CertValidity Period	15	optional	Amount of time in years that the root certificate is valid. Default is 15 years.
Starting Port	no default	optional	Starting port number that the profile will use to generate and assign port values. Port values are assigned sequentially from the Starting Port. Do not specify this parameter if you specify Default Ports or Ports File.
Validate Ports	no default	optional	Indicates that the ports should be validated to ensure that they are not already in use. Valid values are true or false. You should use this option if you specify a Ports File.
Windows Admin Password	no default	required	The Windows Administrator password. Required for Windows.
Windows Admin User	no default	required	This is the Windows Administrator user. Required for Windows.

Provision WebSphere 7 StandAlone Profile

Use this workflow to install the WebSphere 7 Base core binaries and, optionally, create a stand-alone profile.

A stand-alone application server works independently—it is not part of a cell and does not interact with a deployment manager. The stand-alone profile is not suitable for distributed application server environments.

To use this workflow in your environment, see the following information:

Topic	Information Included
"Prerequisites for this Workflow"	List of prerequisites that must be satisfied before you can run this workflow
"How this Workflow Works"	Information about what the workflow does, including validation checks performed, steps executed, and a high-level process flow
"How to Run this Workflow"	Instructions for running this workflow in your environment
"Sample Scenario"	Examples of typical parameter values for this workflow
Parameters	List of input parameters for this workflow

Prerequisites for this Workflow

Be sure that the following prerequisites are satisfied before you run the Provision WebSphere 7 StandAlone Profile workflow:

1. This workflow requires unchallenged `sudo` access to a user (typically `root`) who can access all required files and directories.
2. Per the WebSphere 7 documentation, the following system libraries are required before provisioning IBM WebSphere Application Server version 7 on 64-bit Red Hat Linux:

Platform	Required Library
64-bit Red Hat Enterprise Linux version 5	compat-libstdc++-33-3.2.3-61 compat-db-4.2.52-5.1 libXp-1.0.0-8 compat-libstdc++-296-2.96-138 rpm-build-4.4.2-37.el5

Make sure that these libraries exist on each target server before running this workflow. If newer versions of these libraries are available, you can install the newer versions.

3. This workflow will install WebSphere Application Server as `root` because of the following IBM documented limitations:
 - Creation of a Linux service for WebSphere Application Server
 - Native registration with the operating system
 - Port conflicts that may occur with other installations of WebSphere Application Server that are not registered with the operating system

If there is a need to run as a non-root user after installation, you can run a recursive `chown` under the installation root and set owner permissions accordingly.

For more information about prerequisites for WebSphere 7, refer to the [WebSphere 8 Product Documentation](#).

How this Workflow Works

This topic contains the following information about the Provision WebSphere 7 StandAlone Profile workflow:

Overview

This workflow does the following things in the order shown:

1. Prepares and validates all parameters and creates the call wrapper that will be used to execute commands within a WebSphere 7 environment
2. Checks the documented library requirements, files system space requirements, and temporary space requirements
3. Checks whether the WebSphere 7 binaries are available—if not, they will be downloaded from the software repository—and extracts the binary files from the compressed archive
4. Creates a new response file
5. Provisions IBM WebSphere Application Server version 7 on a target machine
6. Creates a stand-alone profile
7. Starts the stand-alone WebSphere Application Server V7.0

Validation Checks Performed

Most of the validation centers on special characters and spaces in the parameters. There are also validation checks that happen at the operating system level, including file system space checks and RPM checks for Red Hat Linux.

The workflow first performs the following parameter checks:

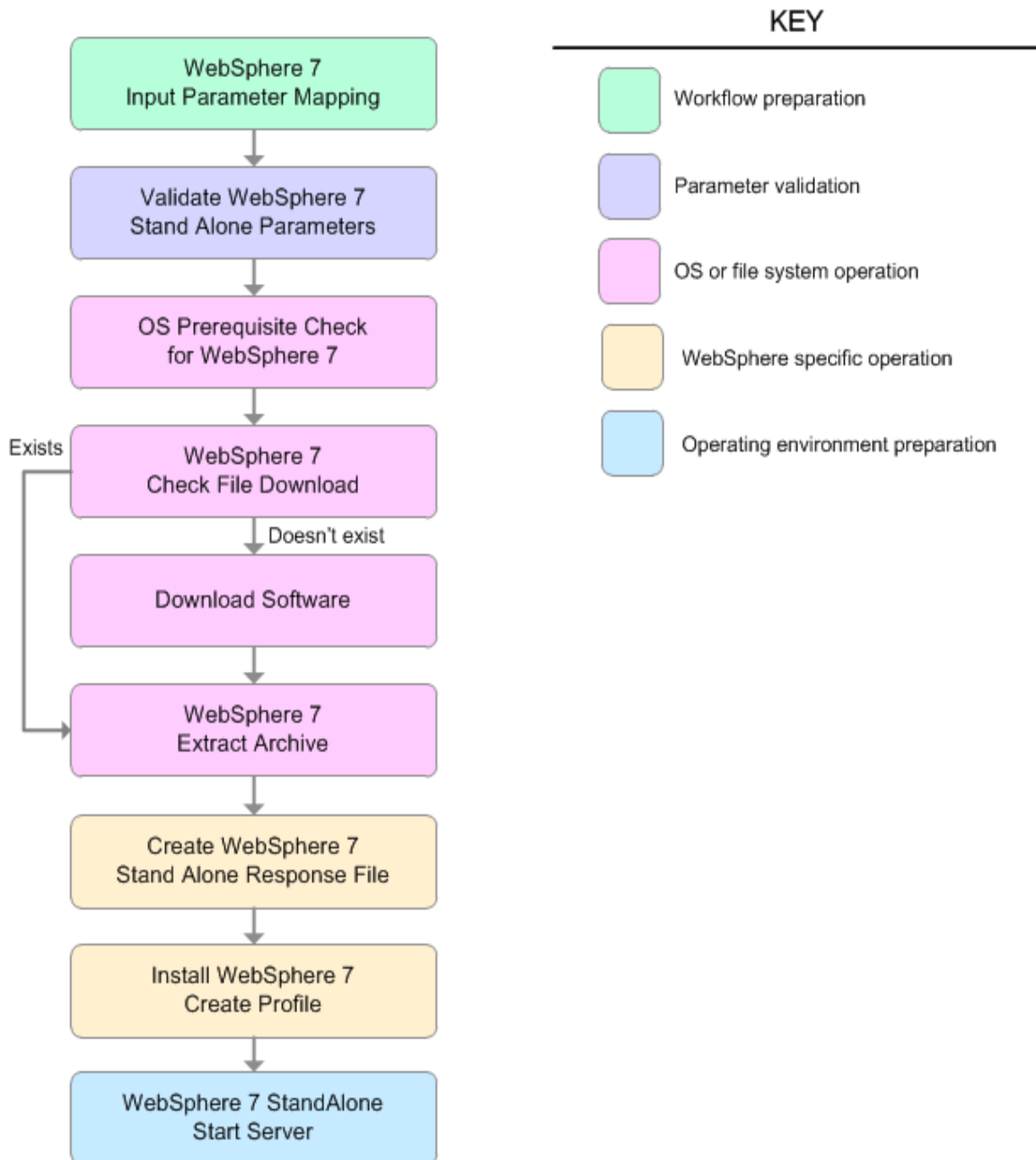
1. Binary Archive is specified. It either exists or can be created successfully.
2. Extract Path and Install Location either exist or can be created successfully.
3. Admin User (if specified) does not begin with a period (.), hyphen (-) or space. It does not contain any of the following characters: / \ * , ; = + ? | < > & % ' " [] # \$ ^ { }
4. Admin Password (if specified) does not begin with a hyphen (-) or contain a space.
5. Cell Name, Node Name, Profile Name, and Server Name are specified. They do not contain the following characters: / \ * , ; = + ? | < > & % ' " [] # \$ ^ { } or space. They do not begin with a period.
6. Host Name is specified.
7. Default Ports and Developer Server (if specified) are true or false.
8. Enable Security is true or false. If Enable Security is true, Admin Password and Admin User are specified.
9. License Acceptance is true.
10. Omit Action (if specified) is defaultAppDeployAndConfig, or deployAdminConsole.
11. Ports File (if specified) exists and Validate Ports is true or false.
12. Starting Port (if specified) is an integer.
13. If the operating system is Windows, Windows Admin User and Windows Admin Password are specified.
14. Profile Path and Response File are specified.
15. Profile Type is standAlone.

The workflow then performs the following operating system checks on the target machine:

1. All required libraries are present (see ["Prerequisites for this Workflow" on page 1242](#)).
2. Sufficient disk space is available to install WebSphere 7.
3. Sufficient disk space is available to extract the binary files from the compressed archive.

Steps Executed

The Provision WebSphere 7 StandAlone Profile workflow includes the following steps. Each step must complete successfully before the next step can start. If a step fails, the workflow reports a failure, and all subsequent steps are skipped.



Steps Used in the Provision WebSphere 7 StandAlone Profile Workflow

Workflow Step	Description
WebSphere 7 Input Parameter Mapping	This step creates the call wrapper—the command that executes the step as a specific user—and allows certain parameters to be hidden or exposed.
Validate WebSphere 7 Stand Alone Parameters	This step prepares and validates the parameters needed to install WebSphere Application Server V7.0 and create a stand-alone profile.
OS Prerequisite Check for WebSphere 7	This step checks the documented library requirements, files system space requirements, and temporary space requirements for WebSphere Application Server V7.0.
WebSphere 7 Check File Download	This step checks for the existence of a file before downloading it from the software repository: <ul style="list-style-type: none"> • Checks if a file exists in the expected location. • If the file is not in the expected location, the file is added to a list of files that need to be downloaded.
Download Software	This step downloads a list of files to a specified location on the target server.
WebSphere 7 Extract Archive	This step checks that the archive file exists and then, based on the archive extension, extracts the archive to the specified directory.
Create WebSphere 7 Stand Alone Response File	This step creates a new response file for installing a new instance of WebSphere Application Server V7.0 and creating a stand-alone profile.
Install WebSphere 7 Create Profile	This step installs a new instance of WebSphere Application Server V7.0 using the <code>install -options <responsefile> silent</code> option and then creates a profile.
WebSphere 7 StandAlone Start Server	This step starts the stand-alone WebSphere Application Server V7.0.

For parameter descriptions and defaults, see ["Parameters for Provision WebSphere 7 StandAlone Profile" on page 1253](#).

How to Run this Workflow

The following instructions show you how to customize and run the Provision WebSphere 7 StandAlone Profile in your environment.

The workflow provides default values for some parameters. These default values are usually sufficient for a "typical" installation. You can override the defaults by specifying parameter values in the deployment. You can also expose additional parameters in the workflow, if necessary, to accomplish more advanced scenarios. Any parameters not explicitly specified in the deployment will have the default values listed in ["Parameters for Provision WebSphere 7 StandAlone Profile" on page 1253](#).

Note: Before following this procedure, review the ["Prerequisites for this Workflow"](#), and ensure that all requirements are satisfied.

To customize and run the Provision WebSphere 7 StandAlone Profile workflow:

1. Create a deployable copy of the workflow.
2. Determine the values that you will specify for the following parameters:

Input Parameters for Validate WebSphere 7 Stand Alone Parameters

Parameter Name	Default Value	Required	Description
Admin Password	no default	optional	When Enable Security is set to true, this parameter must contain a string that does not begin with a dash(-) or contain a space().
Admin User	no default	optional	When Enable Security is set to true, this parameter must contain a string that does not begin with a dash(-), a period(.), or a space(). It cannot contain any of the following characters / \ * , ; = + ? < > & % ' " [] # \$ ^ { }.
Binary Archive	no default	required	Fully qualified path to the compressed software package on the target machine. For example: /opt/install/C1G36ML.tar.gz
Cell Name	no default	required	Unique cell name that does not contain any of the following special characters / \ * , ; = + ? < > & % ' " [] # \$ ^ { }. If you plan to federate into an existing cell later, make sure that this name is not the same as the existing cell name.
Enable Security	no default	required	Enables administrative security. Must be set to either true or false. If Enable Security is true, the Admin User and Admin Password parameters must have values.
Extract Dir	no default	required	Fully qualified path where the compressed

Input Parameters for Validate WebSphere 7 Stand Alone Parameters, continued

Parameter Name	Default Value	Required	Description
			software will be extracted on the target machine.
Install Location	no default	required	Fully qualified path where WebSphere Application Server will be installed. For example: /opt/IBM/WebSphere/AppServer
License Acceptance	false	required	Acknowledges that the end user agrees to the IBM International Program License Agreement. This is set to false by default and must be set to true in order for the installation to continue.
Node Name	no default	required	Unique node name that cannot contain any of the following special characters / \ * , ; ; = + ? < > & % ' " [] # \$ ^ { }. If you plan to federate into an existing cell later, make sure that the name is unique within that cell.
Profile Name	no default	required	A unique profile name. It cannot begin with a period (.) and cannot contain any of the following special characters / \ * , ; ; = + ? < > & % ' " [] # \$ ^ { }.
Profile Path	no default	required	Fully qualified path to the stand-alone profile. For example: /opt/IBM/WebSphere/AppServer/ profiles/AppServer1
Profile Type	standAlone	required	Because this workflow creates a stand-alone profile, the value is standAlone.
Response File	no default	required	Fully qualified path where the response file that this workflow creates will be located. This file will then be used to drive the installation and profile creation.
Server Name	no default	required	Name of the application server that will be created under the profile.
Windows Admin Password	no default	required	The Windows Administrator password. Required for Windows.
Windows Admin User	no default	required	This is the Windows Administrator user. Required for Windows.

Note: This is the minimum set of parameters required to run this workflow. You may need to expose additional parameters depending on your provisioning objectives.

See ["Parameters for Provision WebSphere 7 StandAlone Profile" on page 1253](#) for detailed descriptions of all input parameters for this workflow, including default values.

Tip: To avoid having to re-enter passwords whenever they change, you can create a policy to provide them to the workflow.

3. In the workflow editor, expose any additional parameters that you need. You will specify values for those parameters when you create the deployment.
4. Save the changes to the workflow (click **Save** in the lower right corner).
5. Create a new deployment.
6. On the Parameters tab, specify values for the required parameters listed in step 2 and any additional parameters that you have exposed. You do not need to specify values for those parameters whose default values are appropriate for your environment.
7. On the Targets tab, specify one or more targets for this deployment.
8. Save the deployment (click **Save** in the lower right corner).
9. Run the workflow using this deployment.

To verify the results:

The workflow will complete and report SUCCESS on the Console if it has run successfully. If an error occurs during workflow execution, the error is logged, and the workflow terminates in the FAILURE state.

Optional: if you want to further verify the results, perform the following steps:

1. After the workflow has completed, run the following command to check the version of WebSphere Application Server that was installed:

```
WAS_ROOT/bin/versionInfo.sh
```

Here, *WAS_ROOT* is the directory where WebSphere 7 is installed. This is the path that you specified in the WebSphere Install Location parameter.

2. Validate that stand-alone profile has been created and is running by doing the following:
 - a. View the *WAS_ROOT*/profiles/*PROFILE_NAME*/logs/AboutThisProfile.txt file. This file is created after the creation of the profile and contains specific information about the profile.

Here, *PROFILE_NAME* is the name of the profile that you just created. This is the name that you specified in the Profile Name parameter.

- b. Change to the *WAS_ROOT*/profiles/*PROFILE_NAME*/logs/*SERVER_NAME* directory, and tail the SystemOut.log file. Look for the following line:

```
Server SERVER_NAME open for e-business
```

Here, *SERVER_NAME* is the name of the application server that you just created. This is the name that you specified in the Server Name parameter.

Sample Scenario

This topic shows you typical parameter values used for the Provision WebSphere 7 StandAlone Profile workflow.

New WebSphere 7 install with stand-alone profile

Input Parameters for Validate WebSphere 7 Stand Alone Parameters

Parameter Name	Example Value	Description
Admin Password	wasPassWord	When Enable Security is set to true, this parameter must contain a string that does not begin with a dash(-) or contain a space().
Admin User	wasadmin	When Enable Security is set to true, this parameter must contain a string that does not begin with a dash(-), a period(.), or a space(). It cannot contain any of the following characters <code>/\ * , ; = + ? < > & % ' " [] # \$ ^ { }</code> .
Binary Archive	see description	Fully qualified path to the compressed software package on the target machine. For example: <code>/opt/install/C1G36ML.tar.gz</code>
Cell Name	DevCell	Unique cell name that does not contain any of the following special characters <code>/\ * , ; = + ? < > & % ' " [] # \$ ^ { }</code> . If you plan to federate into an existing cell later, make sure that this name is not the same as the existing cell name.
Enable Security	true	Enables administrative security. Must be set to either true or false. If Enable Security is true, the Admin User and Admin Password parameters must have values.
Extract Dir	<code>/opt/IBM/wasv7</code>	Fully qualified path where the compressed software will be extracted on the target machine.
Install Location	see description	Fully qualified path where WebSphere Application Server will be installed. For example: <code>/opt/IBM/WebSphere/AppServer</code>
License Acceptance	true	Acknowledges that the end user agrees to the IBM International Program License Agreement. This is set to false by default and must be set to true in order for the installation to continue.
Node Name	DevStandAlone1Node	Unique node name that cannot contain any of the following special characters <code>/\ * , ; = + ? < > & % ' " [] # \$ ^ { }</code> . If you plan to federate into an existing cell later, make sure that the name is unique within that cell.
Profile Name	StandAlone1	A unique profile name. It cannot begin with a period (.) and cannot contain any of the following special characters <code>/\ * , ; = + ? < > & % ' " [] # \$ ^ { }</code> .
Profile Path	see description	Fully qualified path to the stand-alone profile. For example: <code>/opt/IBM/WebSphere/AppServer/profiles/AppServer1</code>

Input Parameters for Validate WebSphere 7 Stand Alone Parameters, continued

Parameter Name	Example Value	Description
Profile Type	standAlone	Because this workflow creates a stand-alone profile, the value is standAlone.
Response File	/tmp/serverrsp	Fully qualified path where the response file that this workflow creates will be located. This file will then be used to drive the installation and profile creation.
Server Name	Server1	Name of the application server that will be created under the profile.

Parameters for Provision WebSphere 7 StandAlone Profile

The following tables describe the required and optional input parameters for this workflow. Some of these parameters may not be initially visible in a deployment. For some parameters, if you do not specify a value for a parameter, a default value is assigned.

Parameters Defined in this Step: Validate WebSphere 7 Stand Alone Parameters

Parameter Name	Default Value	Required	Description
Admin Password	no default	optional	When Enable Security is set to true, this parameter must contain a string that does not begin with a dash(-) or contain a space().
Admin User	no default	optional	When Enable Security is set to true, this parameter must contain a string that does not begin with a dash(-), a period (.), or a space(). It cannot contain any of the following characters / \ * , : ; = + ? < > & % ' " [] # \$ ^ { }.
Binary Archive	no default	required	Fully qualified path to the compressed software package on the target machine. For example: /opt/install/C1G36ML.tar.gz
Call Wrapper	see description	required	Command that will execute this step (or subsequent steps) as a specific user. For UNIX targets, the default is: /opt/hp/dma/client/jython.sh running as root For Windows targets, the default is: jython running as Administrator <div>This parameter is derived by the workflow. Under most circumstances, you should not change its mapping or its value.</div>
Cell Name	no default	required	Unique cell name that does not contain any of the following special characters / \ * , : ; = + ? < > & % ' " [] # \$ ^ { }. If you plan to federate into an existing cell later, make sure that this name is not the same as the existing cell name.
Default Ports	false	optional	Provides the option to assign default ports to a profile. Valid values are true or false. If true, the WebSphere Application Server default ports will be used, and the Ports File and Starting Port parameters should not have values. If false, the workflow will increment the default port until it finds a free port. The default value is false.
Developer Server	no default	optional	Use this parameter for development environments only to help with start up time. Valid value is true. Do not use in production environments.
Enable Security	no default	required	Enables administrative security. Must be set to either true or false. If Enable Security is true, the Admin User and Admin Password parameters must have values.

Parameters Defined in this Step: Validate WebSphere 7 Stand Alone Parameters, continued

Parameter Name	Default Value	Required	Description
Extract Dir	no default	required	Fully qualified path where the compressed software will be extracted on the target machine.
Host Name	Server.name	required	Hostname or IP address of the target machine.
Install Location	no default	required	Fully qualified path where WebSphere Application Server will be installed. For example: /opt/IBM/WebSphere/AppServer
Keystore Password	no default	optional	Sets the password for all keystore files created during profile creation. This includes keystore files for both the default personal certificate and the root signing certificate.
License Acceptance	false	required	Acknowledges that the end user agrees to the IBM International Program License Agreement. This is set to false by default and must be set to true in order for the installation to continue.
Node Name	no default	required	Unique node name that cannot contain any of the following special characters / \ * , ; = + ? < > & % ' " [] # \$ ^ { }. If you plan to federate into an existing cell later, make sure that the name is unique within that cell.
Omit Action	no default	optional	Enables you to prevent certain optional features from being installed. Valid values are deployAdminConsole or defaultAppDeployAndConfig. You may only specify one of these options.
Personal CertDN	no default	optional	Distinguished name of the personal certificate. For example: CN=dmalab-example.com,OU=WAS7LabCell,OU=WAS7LabDmgrManager,O=IBM,C=US The DN string cannot contain spaces. If you do not specify the DN, the WebSphere Application Server installer will create one.
Personal CertValidity Period	1	optional	Amount of time in years that the personal certificate is valid. Default is one year.
Ports File	no default	optional	Fully qualified path to a file that defines port settings for the new profile. This file must contain key=value pairs that specify a service name and a port number (for example: WC_adminhost=9060). This option should be used with the Validate Ports option.
Profile Name	no default	required	A unique profile name. It cannot begin with a period (.) and cannot contain any of the following special characters / \ * , ; = + ? < > & % ' " [] # \$ ^ { }.
Profile Path	no default	required	Fully qualified path to the stand-alone profile. For example: /opt/IBM/WebSphere/AppServer/ profiles/AppServer1
Profile Type	standAlone	required	Because this workflow creates a stand-alone profile, the

Parameters Defined in this Step: Validate WebSphere 7 Stand Alone Parameters, continued

Parameter Name	Default Value	Required	Description
			value is standAlone.
Response File	no default	required	Fully qualified path where the response file that this workflow creates will be located. This file will then be used to drive the installation and profile creation.
Server Name	no default	required	Name of the application server that will be created under the profile.
Signing CertDN	no default	optional	Distinguished name of the signing certificate. For example: CN=dmlab-example.com, OU=Root Certificate, OU=WAS7TestLabCell, OU=WAS7LabNode1, O=IBM, C=US The DN string cannot contain spaces. If you do not specify the DN, the WebSphere Application Server installer will create one.
Signing CertValidity Period	15	optional	Amount of time in years that the root certificate is valid. Default is 15 years.
Starting Port	no default	optional	Starting port number that the profile will use to generate and assign port values. Port values are assigned sequentially from the Starting Port. Do not specify this parameter if you specify Default Ports or Ports File.
Validate Ports	no default	optional	Indicates that the ports should be validated to ensure that they are not already in use. Valid values are true or false. You should use this option if you specify a Ports File.
Windows Admin Password	no default	required	The Windows Administrator password. Required for Windows.
Windows Admin User	no default	required	This is the Windows Administrator user. Required for Windows.

Provision IBM HTTP Server 7 and Plug-In

Use this workflow to install IBM HTTP Server for WebSphere Application Server V7.0 and, optionally, install its WebSphere Application Server Plug-In.

To use this workflow in your environment, see the following information:

Topic	Information Included
"Prerequisites for this Workflow"	List of prerequisites that must be satisfied before you can run this workflow
"How this Workflow Works"	Information about what the workflow does, including validation checks performed, steps executed, and a high-level process flow
"How to Run this Workflow"	Instructions for running this workflow in your environment
"Sample Scenario"	Examples of typical parameter values for this workflow
Parameters	List of input parameters for this workflow

Prerequisites for this Workflow

Be sure that the following prerequisites are satisfied before you run the Provision IBM HTTP Server 7 and Plug-In workflow:

1. This workflow requires unchallenged `sudo` access to a user (typically `root`) who can access all required files and directories.
2. Per the WebSphere 7 documentation, the following system libraries are required before provisioning IBM WebSphere Application Server version 7 on 64-bit Red Hat Linux:

Platform	Required Library
64-bit Red Hat Enterprise Linux version 5	compat-libstdc++-33-3.2.3-61 compat-db-4.2.52-5.1 libXp-1.0.0-8 compat-libstdc++-296-2.96-138 rpm-build-4.4.2-37.el5

Make sure that these libraries exist on each target server before running this workflow. If newer versions of these libraries are available, you can install the newer versions.

3. This workflow will install WebSphere Application Server as `root` because of the following IBM documented limitations:
 - Creation of a Linux service for WebSphere Application Server
 - Native registration with the operating system
 - Port conflicts that may occur with other installations of WebSphere Application Server that are not registered with the operating system

If there is a need to run as a non-root user after installation, you can run a recursive `chown` under the installation root and set owner permissions accordingly.

For more information about prerequisites for WebSphere 7, refer to the [WebSphere 7 Product Documentation](#).

How this Workflow Works

This topic contains the following information about the Provision IBM HTTP Server 7 and Plug-In workflow:

Overview

This workflow does the following things in the order shown:

1. Prepares and validates all parameters and creates the call wrapper that will be used to execute commands within a WebSphere 7 environment
2. Checks the documented library requirements, files system space requirements, and temporary space requirements
3. Checks whether the WebSphere 7 binaries are available—if not, they will be downloaded from the software repository—and extracts the binary files from the compressed archive
4. Creates a new response file for installing IBM HTTP Server and creating its plug-in
5. Installs IBM HTTP Server

Validation Checks Performed

Most of the validation centers on special characters and spaces in the parameters. There are also validation checks that happen at the operating system level, including file system space checks and RPM checks for Red Hat Linux.

The workflow first performs the following parameter checks:

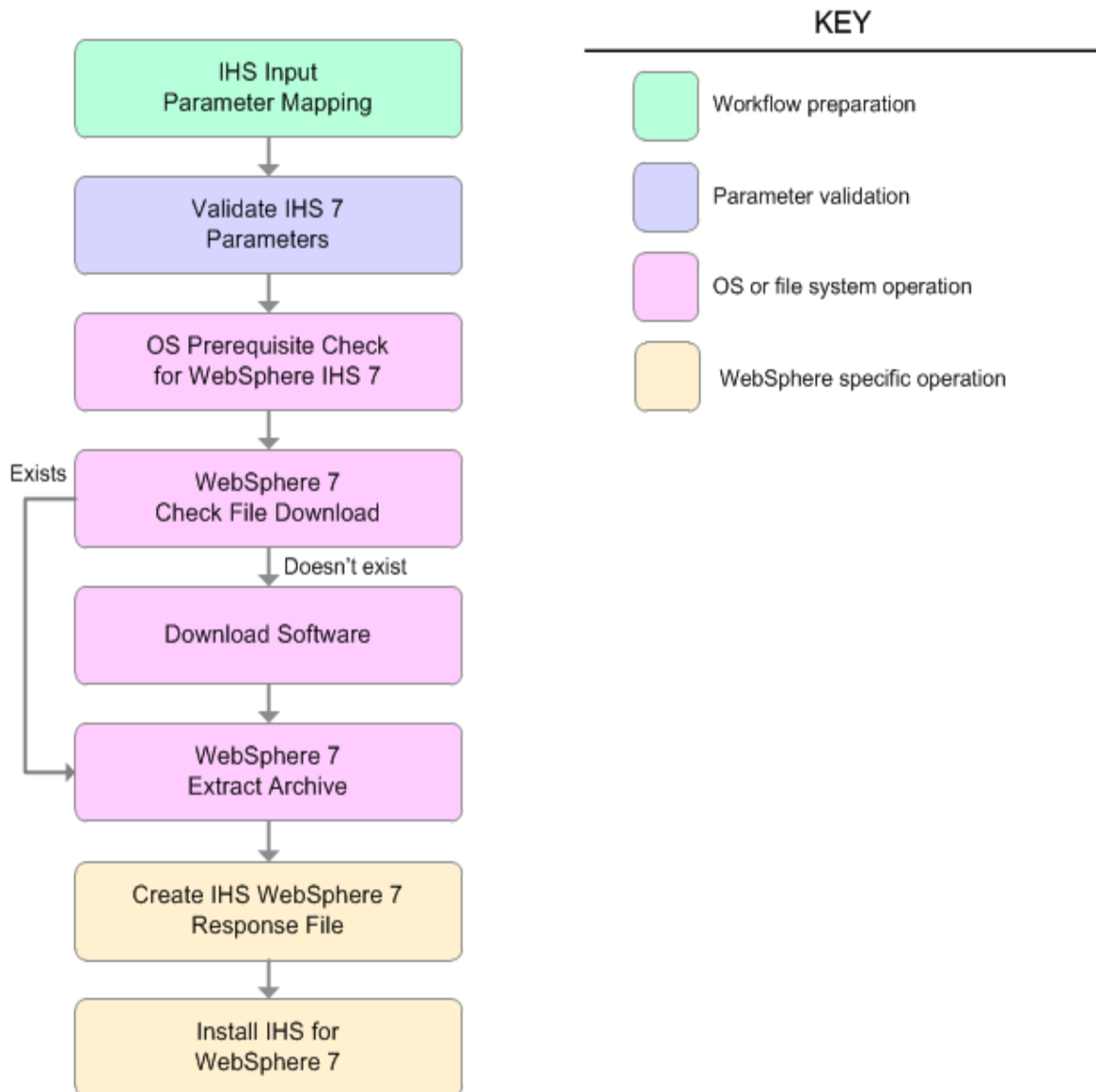
1. If Create Admin Auth is true, Admin Auth User, Admin Auth Password, and Admin Auth Password Confirm are specified.
2. If Create Admin User Group is true, Set Up Admin User and Set Up Admin Group are specified.
3. If Install Plugin is true, WebSphere Hostname is specified.
4. Binary Archive is a full file path. The directory path either exists or can be created successfully.
5. Extract Dir and Install Location are full directory paths. The directory paths either exist or can be created successfully.
6. Admin Auth User does not contain a colon (:).
7. Webserver Definition and WebSphere Hostname do not contain a space ().
8. Http Port and Admin Port (if specified) are integers.
9. License Acceptance, Create Admin Auth, Run Admin Setup, Create Admin User Group, and Install Plugin are true or false (case insensitive).

The workflow then performs the following operating system checks on the target machine:

1. All required libraries are present (see ["Prerequisites for this Workflow" on page 1257](#)).
2. Sufficient disk space is available to install IBM HTTP Server for WebSphere Application Server V7.0.
3. Sufficient disk space is available to extract the binary files from the compressed archive.

Steps Executed

The Provision IBM HTTP Server 7 and Plug-In workflow includes the following steps. Each step must complete successfully before the next step can start. If a step fails, the workflow reports a failure, and all subsequent steps are skipped.



Steps Used in the Provision IBM HTTP Server 7 and Plug-In Workflow

Workflow Step	Description
IHS Input Parameter Mapping	This step allows for either the defaulting of parameters to be used later in a step or to hide or expose certain parameters that will or will not be needed depending on what the end user wants to do.
Validate IHS 7 Parameters	This step prepares and validates the parameters needed to install IBM HTTP Server for WebSphere Application Server V7.0 and, optionally, create its WebSphere Application Server plug-in.
OS Prerequisite Check for WebSphere IHS 7	<p>This step checks the following:</p> <ol style="list-style-type: none"> 1. Documented library requirements for WebSphere Application Server V7.0. 2. Files system space requirements where IBM HTTP Server for WebSphere Application Server V7.0 will be installed.. 3. Temporary space requirements where the compressed software will be extracted before it is installed.
WebSphere 7 Check File Download	<p>This step checks for the existence of a file before downloading it from the software repository:</p> <ul style="list-style-type: none"> • Checks if a file exists in the expected location. • If the file is not in the expected location, the file is added to a list of files that need to be downloaded.
Download Software	This step downloads a list of files to a specified location on the target server.
WebSphere 7 Extract Archive	This step checks that the archive file exists and then, based on the archive extension, extracts the archive to the specified directory.
Create IHS WebSphere 7 Response File	This step creates a new response file for installing IBM HTTP Server for WebSphere Application Server V7.0 and then, optionally, creating its WebSphere Application Server plug-in.
Install IHS for WebSphere 7	This step installs IBM HTTP Server for WebSphere Application Server V7.0 using the "install -options <responsefile> silent" option.

How to Run this Workflow

The following instructions show you how to customize and run the Provision IBM HTTP Server 7 and Plug-In workflow in your environment.

Note: Before following this procedure, review the ["Prerequisites for this Workflow"](#), and ensure that all requirements are satisfied.

To customize and run the Provision IBM HTTP Server 7 and Plug-In workflow:

1. Create a deployable copy of the workflow.
2. Determine the values that you will specify for the following parameters:

Input Parameters for Validate IHS 7 Parameters

Parameter Name	Default Value	Required	Description
Admin Auth Password	no default	optional	The password used to authenticate to the IBM HTTP administration server using the WebSphere Application Server administrative console. When Create Admin Auth is set to true, this parameter must have a value. It cannot begin with a dash(-) or contain a space().
Admin Auth Password Confirm	no default	optional	Confirms the Admin Auth Password.
Admin Auth User	no default	optional	The user ID used to authenticate to the IBM HTTP administration server using the WebSphere Application Server administrative console. When Create Admin Auth is set to true, this parameter must have a value. It cannot begin with a dash(-), a period(.), or a space() and cannot contain any of the following characters / \ * , ; = + ? < > & % ' " [] # \$ ^ { }
Admin Port	no default	required	The port on which the HTTP administration web server will run. This is usually 8008.
Binary Archive	no default	required	Fully qualified path to the compressed software package on the target machine. For example: /opt/install/C1G36ML.tar.gz
Create Admin Auth	no default	required	Set this to true to create a user ID and password to authenticate to the IBM HTTP administration server using the WebSphere Application Server administrative console. If this parameter is set to true, the following parameters must have values: Admin Auth Password, Admin Auth Password Confirm, and Admin Auth User.
Create Admin User Group	no default	required	Set to true to create a user ID and group used to set up the IBM HTTP Administration Server on Linux and UNIX operating systems.

Input Parameters for Validate IHS 7 Parameters, continued

Parameter Name	Default Value	Required	Description
Extract Dir	no default	required	Fully qualified path where the compressed software will be extracted on the target machine.
Http Port	no default	required	The port on which the web server will listen. This is usually set to 80.
Install Location	no default	required	Fully qualified path where IBM HTTP Server will be installed. For example: /opt/IBM/HTTPServer
Install Plugin	no default	required	Determines whether or not the WebSphere Application Server Plug-In is installed. Valid options are true or false.
License Acceptance	false	required	Acknowledges that the end user agrees to the IBM International Program License Agreement. This is set to false by default and must be set to true in order for the installation to continue.
Response File	no default	required	Fully qualified path where the response file that this workflow creates will be located. This file is used to drive the installation.
Run Admin Setup	no default	required	Enables the install process to grant the Set Up Admin User write access to the necessary IBM HTTP Server and WebSphere Application Server Plug-In configuration files. Valid options are true or false.
Set Up Admin Group	no default	optional	Group name used to set up the IBM HTTP administration server on Linux and UNIX operating systems. This parameter must have a value if Create Admin User Group is set to true.
Set Up Admin User	no default	optional	User ID used to set up the IBM HTTP administration server on Linux and UNIX operating systems. If Create Admin User Group is set to true, this parameter must have a value.
Webserver Definition	no default	optional	A web server definition allows for web server administration through the WebSphere administrative console. This parameter must be set if the Install Plugin parameter is set to true. An example would be webserver1. No spaces are allowed in the Webserver Definition name.
WebSphere Hostname	no default	optional	Host name of the WebSphere Application Server machine. This parameter is required if Install Plugin is set to true. No spaces are allowed in the host name.

Additional Input Parameters for Install IHS for WebSphere 7

Parameter Name	Default Value	Required	Description
Password	no default	required	The Windows Administrator password. Required for Windows.

Additional Input Parameters for Install IHS for WebSphere 7, continued

Parameter Name	Default Value	Required	Description
Username	no default	required	This is the Windows Administrator user. Required for Windows.

Note: See "[Parameters for Provision IBM HTTP Server 7 and Plug-in](#)" for detailed descriptions of all input parameters for this workflow, including default values.

Tip: To avoid having to re-enter passwords whenever they change, you can create a policy to provide them to the workflow.

3. Save the changes to the workflow (click **Save** in the lower right corner).
4. Create a new deployment.
5. On the Parameters tab, specify values for the required parameters listed in step 2.
6. On the Targets tab, specify one or more targets for this deployment.
7. Save the deployment (click **Save** in the lower right corner).
8. Run the workflow using this deployment.

To verify the results:

The workflow will complete and report SUCCESS on the Console if it has run successfully. If an error occurs during workflow execution, the error is logged, and the workflow terminates in the FAILURE state.

Optional: if you want to further verify the results, perform the following steps:

1. After the workflow has completed, run the following command to check the version IBM HTTP Server that was installed:

```
IHS_ROOT/bin/versionInfo.sh
```

Here, *IHS_ROOT* is the directory where IBM HTTP Server is installed. This is the path that you specified in the WebSphere Install Location parameter.

2. Validate that the IBM HTTP Server has been properly installed by doing the following:

View the *IHS_ROOT*/logs/install/log.txt file.

If the installation was successful, you should see messages similar to these:

```
(Apr 21, 2011 9:21:06 AM), Process,  
com.ibm.ws.install.ni.ismp.actions.SettleNIFRegistryAction, msg1, Current  
install/uninstall process is successful. Process type is: install
```

```
(Apr 21, 2011 9:21:07 AM), Process,  
com.ibm.ws.install.ni.ismp.actions.SetExitCodeAction, msg1, CWUPI0000I:  
EXITCODE=0
```

```
(Apr 21, 2011 9:21:07 AM), Process,  
com.ibm.ws.install.ni.ismp.actions.ISMPLogSuccessMessageAction, msg1,  
INSTCONFSUCCESS
```

3. If you installed the WebSphere Application Server Plug-In, validate that it has been properly installed by doing the following:

View the *IHS_ROOT*/Plugins/logs/install/log.txt file.

If the installation was successful, you should see messages similar to these:

```
(Apr 21, 2011 9:21:05 AM), Process,  
com.ibm.ws.install.ni.ismp.actions.ISMPLogFileAction, msg1, INSTCONF_COMPLETE :  
Installation is complete.
```

```
(Apr 21, 2011 9:21:05 AM), Process,  
com.ibm.ws.install.ni.ismp.actions.ISMPLogFileAction, msg1,  
*****
```



```
(Apr 21, 2011 9:21:05 AM), Process,  
com.ibm.ws.install.ni.ismp.actions.SetExitCodeAction, msg1, CWUPI0000I:  
EXITCODE=0
```

```
(Apr 21, 2011 9:21:05 AM), Process,  
com.ibm.ws.install.ni.ismp.actions.ISMPLogSuccessMessageAction, msg1,  
INSTCONFSUCCESS
```

Sample Scenario

This topic shows you typical parameter values used for the Provision IBM HTTP Server 7 and Plug-In workflow.

Scenario 1: New IBM HTTP Server install with plug-in using the simplest method

This example shows the following:

Task	Parameter Values
Do not create a user ID and password to authenticate to the IBM HTTP administration server using the WebSphere Application Server administrative console	<ul style="list-style-type: none"> Set Create Admin Auth to false
Do not create a user ID and group used to set up the IBM HTTP Administration Server on Linux and UNIX operating systems	<ul style="list-style-type: none"> Set Create Admin User Group to false
Do not install the WebSphere Application Server Plug-In	<ul style="list-style-type: none"> Set Install Plugin to false
Do not grant the Set Up Admin User write access to the necessary IBM HTTP Server and WebSphere Application Server Plug-In configuration files	<ul style="list-style-type: none"> Set Run Admin Setup to false

Input Parameters for Validate IHS 7 Parameters

Parameter Name	Example Value	Description
Admin Port	8008	The port on which the HTTP administration web server will run. This is usually 8008.
Binary Archive	see description	Fully qualified path to the compressed software package on the target machine. For example: /opt/install/C1G36ML.tar.gz
Create Admin Auth	false	Set this to true to create a user ID and password to authenticate to the IBM HTTP administration server using the WebSphere Application Server administrative console. If this parameter is set to true, the following parameters must have values: Admin Auth Password, Admin Auth Password Confirm, and Admin Auth User.
Create Admin User Group	false	Set to true to create a user ID and group used to set up the IBM HTTP Administration Server on Linux and UNIX operating systems.
Extract Dir	/opt/IBM/wasv7	Fully qualified path where the compressed software will be extracted on the target machine.
Http Port	80	The port on which the web server will listen. This is usually set to 80.
Install Location	see description	Fully qualified path where IBM HTTP Server will be installed. For example: /opt/IBM/HTTPServer
Install Plugin	false	Determines whether or not the WebSphere Application Server Plug-In is installed. Valid options are true or false.

Input Parameters for Validate IHS 7 Parameters, continued

Parameter Name	Example Value	Description
License Acceptance	true	Acknowledges that the end user agrees to the IBM International Program License Agreement. This is set to false by default and must be set to true in order for the installation to continue.
Response File	/tmp/serverrsp	Fully qualified path where the response file that this workflow creates will be located. This file is used to drive the installation.
Run Admin Setup	false	Enables the install process to grant the Set Up Admin User write access to the necessary IBM HTTP Server and WebSphere Application Server Plug-In configuration files. Valid options are true or false.

Scenario 2: New IBM HTTP Server install with plug-in using all the options

This example shows the following:

Task	Parameter Values
To create a user ID and password to authenticate to the IBM HTTP administration server using the WebSphere Application Server administrative console	<ul style="list-style-type: none"> Set Create Admin Auth to true Specify values for: Admin Auth Password Admin Auth Password Confirm Admin Auth User
To create a user ID and group used to set up the IBM HTTP Administration Server on Linux and UNIX operating systems	<ul style="list-style-type: none"> Set Create Admin User Group to true Specify values for: Set Up Admin Group Set Up Admin User
To install the WebSphere Application Server Plug-In	<ul style="list-style-type: none"> Set Install Plugin to true Specify values for: WebSphere Hostname Webserver Definition
To grant the Set Up Admin User write access to the necessary IBM HTTP Server and WebSphere Application Server Plug-In configuration files	<ul style="list-style-type: none"> Set Run Admin Setup to true

Input Parameters for Validate IHS 7 Parameters

Parameter Name	Example Value	Description
Admin Auth Password	AdminPsWd	The password used to authenticate to the IBM HTTP administration server using the WebSphere Application Server administrative console. When Create Admin Auth is set to true, this parameter must have a value. It cannot begin with a dash(-) or contain a space().
Admin Auth Password Confirm	AdminPsWd	Confirms the Admin Auth Password.
Admin Auth User	admin	The user ID used to authenticate to the IBM HTTP administration server using the WebSphere Application Server administrative console. When Create Admin Auth is set to true, this parameter must have a value. It cannot begin with a dash(-), a period(.), or a space() and cannot contain any of the following characters / \ * , ; = + ? < > & % ' " [] # \$ ^ { }
Admin Port	8008	The port on which the HTTP administration web server will run. This is usually 8008.
Binary Archive	see description	Fully qualified path to the compressed software package on the target machine. For example: /opt/install/C1G36ML.tar.gz
Create	false	Set to true to create a user ID and group used to set up the

Input Parameters for Validate IHS 7 Parameters, continued

Parameter Name	Example Value	Description
Admin User Group		IBM HTTP Administration Server on Linux and UNIX operating systems.
Extract Dir	/opt/IBM/wasv7	Fully qualified path where the compressed software will be extracted on the target machine.
Http Port	80	The port on which the web server will listen. This is usually set to 80.
Install Location	see description	Fully qualified path where IBM HTTP Server will be installed. For example: /opt/IBM/HTTPServer
Install Plugin	false	Determines whether or not the WebSphere Application Server Plug-In is installed. Valid options are true or false.
License Acceptance	true	Acknowledges that the end user agrees to the IBM International Program License Agreement. This is set to false by default and must be set to true in order for the installation to continue.
Response File	/tmp/serverrsp	Fully qualified path where the response file that this workflow creates will be located. This file is used to drive the installation.
Run Admin Setup	false	Enables the install process to grant the Set Up Admin User write access to the necessary IBM HTTP Server and WebSphere Application Server Plug-In configuration files. Valid options are true or false.
Set Up Admin Group	AdminGrp	Group name used to set up the IBM HTTP administration server on Linux and UNIX operating systems. This parameter must have a value if Create Admin User Group is set to true.
Set Up Admin User	AdminUsr	User ID used to set up the IBM HTTP administration server on Linux and UNIX operating systems. If Create Admin User Group is set to true, this parameter must have a value.
Webserver Definition	webserver1	A web server definition allows for web server administration through the WebSphere administrative console. This parameter must be set if the Install Plugin parameter is set to true. An example would be webserver1. No spaces are allowed in the Webserver Definition name.
WebSphere Hostname	was1.mycompany.com	Host name of the WebSphere Application Server machine. This parameter is required if Install Plugin is set to true. No spaces are allowed in the host name.
Admin Auth Password	AdminPsWd	The password used to authenticate to the IBM HTTP administration server using the WebSphere Application Server administrative console. When Create Admin Auth is set to true, this parameter must have a value. It cannot begin with a dash(-) or contain a space().

Parameters for Provision IBM HTTP Server 7 and Plug-in

The following tables describe the required and optional input parameters for this workflow. For most parameters, if you do not specify a value for a parameter, a default value is assigned.

Note: Only those parameters that are configurable in a standard deployment are listed here. Input parameters that must be mapped to output parameters of previous steps are not listed.

Parameters Defined in this Step: Validate IHS 7 Parameters

Parameter Name	Default Value	Required	Description
Admin Auth Password	default	optional	The password used to authenticate to the IBM HTTP administration server using the WebSphere Application Server administrative console. When Create Admin Auth is set to true, this parameter must have a value. It cannot begin with a dash(-) or contain a space().
Admin Auth Password Confirm	default	optional	Confirms the Admin Auth Password.
Admin Auth User	default	optional	The user ID used to authenticate to the IBM HTTP administration server using the WebSphere Application Server administrative console. When Create Admin Auth is set to true, this parameter must have a value. It cannot begin with a dash(-), a period(.), or a space() and cannot contain any of the following characters / \ * , ; = + ? < > & % ' " [] # \$ ^ { }
Admin Port	default	required	The port on which the HTTP administration web server will run. This is usually 8008.
Binary Archive	default	required	Fully qualified path to the compressed software package on the target machine. For example: /opt/install/C1G36ML.tar.gz
Call Wrapper	see description	required	Command that will execute this step (or subsequent steps) as a specific user. For UNIX targets, the default is: /opt/hp/dma/client/jython.sh running as root For Windows targets, the default is: jython running as Administrator This parameter is derived by the workflow. Under most circumstances, you should not change its mapping or its value.
Create Admin Auth	default	required	Set this to true to create a user ID and password to authenticate to the IBM HTTP administration server using the WebSphere Application Server administrative console. If this parameter is set to true, the following parameters must have values: Admin Auth Password, Admin Auth Password Confirm, and Admin Auth User.

Parameters Defined in this Step: Validate IHS 7 Parameters, continued

Parameter Name	Default Value	Required	Description
Create Admin User Group	default	required	Set to true to create a user ID and group used to set up the IBM HTTP Administration Server on Linux and UNIX operating systems.
Extract Dir	default	required	Fully qualified path where the compressed software will be extracted on the target machine.
Http Port	default	required	The port on which the web server will listen. This is usually set to 80.
Install Location	default	required	Fully qualified path where IBM HTTP Server will be installed. For example: /opt/IBM/HTTPServer
Install Plugin	default	required	Determines whether or not the WebSphere Application Server Plug-In is installed. Valid options are true or false.
License Acceptance	false	required	Acknowledges that the end user agrees to the IBM International Program License Agreement. This is set to false by default and must be set to true in order for the installation to continue.
Response File	default	required	Fully qualified path where the response file that this workflow creates will be located. This file is used to drive the installation.
Run Admin Setup	default	required	Enables the install process to grant the Set Up Admin User write access to the necessary IBM HTTP Server and WebSphere Application Server Plug-In configuration files. Valid options are true or false.
Set Up Admin Group	default	optional	Group name used to set up the IBM HTTP administration server on Linux and UNIX operating systems. This parameter must have a value if Create Admin User Group is set to true.
Set Up Admin User	default	optional	User ID used to set up the IBM HTTP administration server on Linux and UNIX operating systems. If Create Admin User Group is set to true, this parameter must have a value.
Webserver Definition	default	optional	A web server definition allows for web server administration through the WebSphere administrative console. This parameter must be set if the Install Plugin parameter is set to true. An example would be webserver1. No spaces are allowed in the Webserver Definition name.
WebSphere Hostname	default	optional	Host name of the WebSphere Application Server machine. This parameter is required if Install Plugin is set to true. No spaces are allowed in the host name.

Additional Parameters Defined in this Step: Install IHS for WebSphere 7

Parameter Name	Default Value	Required	Description
Password	no default	required	The Windows Administrator password. Required for Windows.

Additional Parameters Defined in this Step: Install IHS for WebSphere 7, continued

Parameter Name	Default Value	Required	Description
Username	no default	required	This is the Windows Administrator user. Required for Windows.

Create StandAlone from Existing WebSphere 7 Install

Use this workflow to create a stand-alone profile on an existing WebSphere 7 installation.

A stand-alone application server works independently—it is not part of a cell and does not interact with a deployment manager. The stand-alone profile is not suitable for distributed application server environments.

This workflow uses the built-in profile management functions (manageprofiles) in IBM WebSphere Application Server version 7 to create a stand-alone profile on top of an existing installation.

To use this workflow in your environment, see the following information:

Topic	Information Included
"Prerequisites for this Workflow"	List of prerequisites that must be satisfied before you can run this workflow
"How this Workflow Works"	Information about what the workflow does, including validation checks performed, steps executed, and a high-level process flow
"How to Run this Workflow"	Instructions for running this workflow in your environment
"Sample Scenario"	Examples of typical parameter values for this workflow
Parameters	List of input parameters for this workflow

Prerequisites for this Workflow

Be sure that the following prerequisites are satisfied before you run the Create StandAlone from Existing WebSphere 7 Install workflow:

1. This workflow requires unchallenged `sudo` access to a user (typically `root`) who can access all required files and directories.
2. Per the WebSphere 7 documentation, the following system libraries are required before provisioning IBM WebSphere Application Server version 7 on 64-bit Red Hat Linux:

Platform	Required Library
64-bit Red Hat Enterprise Linux version 5	compat-libstdc++-33-3.2.3-61 compat-db-4.2.52-5.1 libXp-1.0.0-8 compat-libstdc++-296-2.96-138 rpm-build-4.4.2-37.el5

Make sure that these libraries exist on each target server before running this workflow. If newer versions of these libraries are available, you can install the newer versions.

3. This workflow will install WebSphere Application Server as `root` because of the following IBM documented limitations:
 - Creation of a Linux service for WebSphere Application Server
 - Native registration with the operating system
 - Port conflicts that may occur with other installations of WebSphere Application Server that are not registered with the operating system

If there is a need to run as a non-root user after installation, you can run a recursive `chown` under the installation root and set owner permissions accordingly.

For more information about prerequisites for WebSphere 7, refer to the [WebSphere 8 Product Documentation](#).

How this Workflow Works

This topic contains the following information about the Create StandAlone from Existing WebSphere 7 Install workflow:

Overview

This workflow does the following things in the order shown:

1. Prepares and validates all parameters and creates the call wrapper that will be used to execute commands within a WebSphere 7 environment
2. Creates a new response file
3. Creates a stand-alone profile
4. Starts the stand-alone WebSphere Application Server V7.0

Validation Checks Performed

Most of the validation centers on special characters and spaces in the parameters. There are also validation checks that happen at the operating system level, including file system space checks and RPM checks for Red Hat Linux.

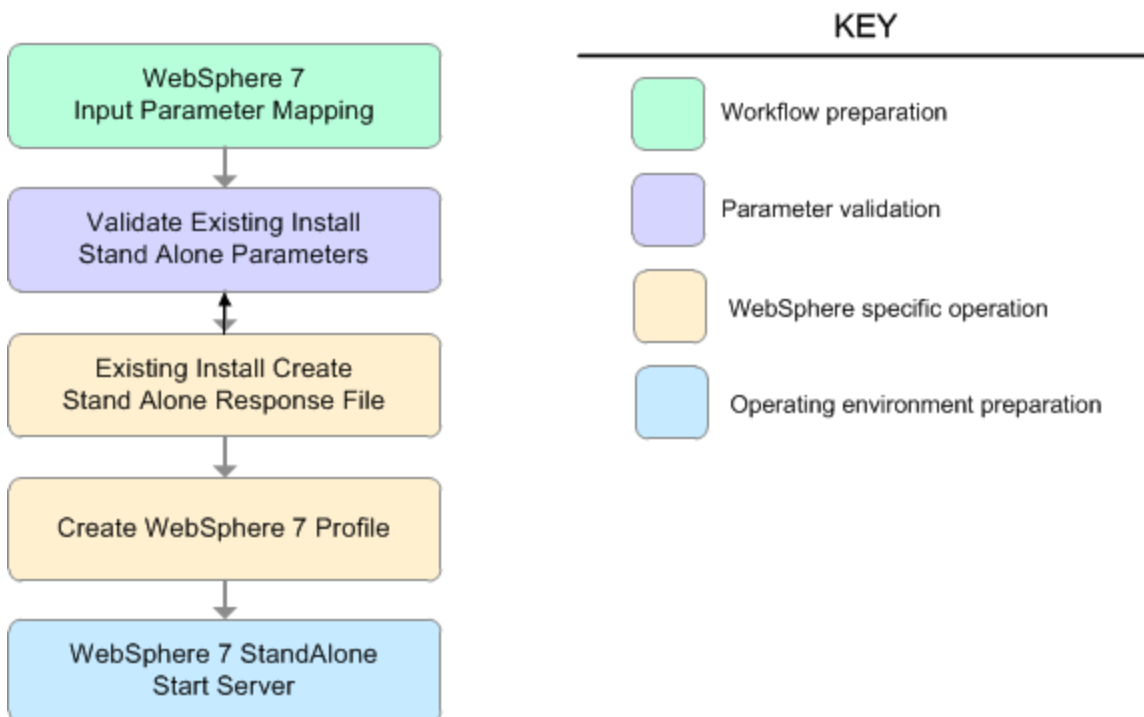
The workflow performs the following parameter checks:

1. Admin User (if specified) does not begin with a period (.), hyphen (-) or space. It does not contain any of the following characters: / \ * , : ; = + ? | < > & % ' " [] # \$ ^ { }
2. Admin Password (if specified) does not begin with a hyphen (-) or contain a space.
3. Cell Name, Node Name, Profile Name, and Server Name are specified. They do not contain the following characters: / \ * , : ; = + ? | < > & % ' " [] # \$ ^ { } or space. They do not begin with a period.
4. Host Name is specified.
5. Default Ports and Developer Server (if specified) are true or false.
6. Enable Security is true or false. If Enable Security is true, Admin Password and Admin User are specified.
7. Omit Action (if specified) is defaultAppDeployAndConfig, or deployAdminConsole.
8. Ports File (if specified) exists and Validate Ports is true or false.
9. Starting Port (if specified) is an integer.

10. Profile Path and Response File are specified.
11. Install Location points to a valid existing WebSphere 7 installation.

Steps Executed

The Create StandAlone from Existing WebSphere 7 Install workflow includes the following steps. Each step must complete successfully before the next step can start. If a step fails, the workflow reports a failure, and all subsequent steps are skipped.



Steps Used in the Create StandAlone from Existing WebSphere 7 Install Workflow

Workflow Step	Description
WebSphere 7 Input Parameter Mapping	This step creates the call wrapper—the command that executes the step as a specific user—and allows certain parameters to be hidden or exposed.
Validate Existing Install Stand Alone Parameters	This step prepares and validates the parameters needed to create a stand-alone profile for an existing WebSphere Application Server V7.0 installation.
Existing Install Create Stand Alone Response File	This step creates a new response file to create a stand-alone profile on top of an existing WebSphere Application Server V7.0 installation.
Create WebSphere 7 Profile	This step creates a profile on top of an existing WebSphere Application Server V7.0

Steps Used in the Create StandAlone from Existing WebSphere 7 Install Workflow, continued

Workflow Step	Description
	installation.
WebSphere 7 StandAlone Start Server	This step starts the stand-alone WebSphere Application Server V7.0.

Sample Scenario

This topic shows you typical parameter values used for the Create StandAlone from Existing WebSphere 7 Install workflow.

Stand-alone profile on Existing Install—Parameter Value Examples

Parameters Defined in this Step: Validate Existing Install Stand Alone Parameters

Parameter Name	Example Value	Description
Admin Password	wasPassWord	When Enable Security is set to true, this parameter must contain a string that does not begin with a dash(-) or contain a space().
Admin User	wasadmin	When Enable Security is set to true, this parameter must contain a string that does not begin with a dash(-), a period(.), or a space(). It cannot contain any of the following characters / \ * , ; ; = + ? < > & % ' " [] # \$ ^ { }.
Cell Name	DevCell	Unique cell name that does not contain any of the following special characters / \ * , ; ; = + ? < > & % ' " [] # \$ ^ { }. If you plan to federate into an existing cell later, make sure that this name is not the same as the existing cell name.
Enable Security	true	Enables administrative security. Must be set to either true or false. If Enable Security is true, the Admin User and Admin Password parameters must have values.
Install Location	see description	Fully qualified path where WebSphere Application Server will be installed. For example: /opt/IBM/WebSphere/AppServer
Node Name	DevStandAlone1Node	Unique node name that cannot contain any of the following special characters / \ * , ; ; = + ? < > & % ' " [] # \$ ^ { }. If you plan to federate into an existing cell later, make sure that the name is unique within that cell.
Profile Name	StandAlone1	A unique profile name. It cannot begin with a period (.) and cannot contain any of the following special characters / \ * , ; ; = + ? < > & % ' " [] # \$ ^ { }.
Profile Path	see description	Fully qualified path to the stand-alone profile. For example: /opt/IBM/WebSphere/AppServer/ profiles/AppServer1
Response File	/tmp/serverrsp	Fully qualified path where the response file that this workflow creates will be located. This file will then be used to drive the installation and profile creation.
Server Name	Server1	Name of the application server that will be created under the profile.

How to Run this Workflow

The following instructions show you how to customize and run the Create StandAlone from Existing WebSphere 7 Install workflow in your environment.

The workflow provides default values for some parameters. These default values are usually sufficient for a "typical" installation. You can override the defaults by specifying parameter values in the deployment. You can also expose additional parameters in the workflow, if necessary, to accomplish more advanced scenarios. Any parameters not explicitly specified in the deployment will have the default values listed in ["Parameters for Create StandAlone from Existing WebSphere 7 Install" on page 1285](#)

Note: Before following this procedure, review the ["Prerequisites for this Workflow"](#), and ensure that all requirements are satisfied.

To customize and run the Create StandAlone from Existing WebSphere 7 Install workflow:

1. Create a deployable copy of the workflow.
2. Determine the values that you will specify for the following parameters:

Input Parameters for Validate Existing Install Stand Alone Parameters

Parameter Name	Default Value	Required	Description
Admin Password	no default	optional	When Enable Security is set to true, this parameter must contain a string that does not begin with a dash(-) or contain a space().
Admin User	no default	optional	When Enable Security is set to true, this parameter must contain a string that does not begin with a dash(-), a period(.), or a space(). It cannot contain any of the following characters / \ * , : ; = + ? < > & % ' " [] # \$ ^ { }.
Cell Name	no default	required	Unique cell name that does not contain any of the following special characters / \ * , : ; = + ? < > & % ' " [] # \$ ^ { }. If you plan to federate into an existing cell later, make sure that this name is not the same as the existing cell name.
Enable Security	no default	required	Enables administrative security. Must be set to either true or false. If Enable Security is true, the Admin User and Admin Password parameters must have values.

Input Parameters for Validate Existing Install Stand Alone Parameters, continued

Parameter Name	Default Value	Required	Description
Install Location	no default	required	Fully qualified path where WebSphere Application Server will be installed. For example: /opt/IBM/WebSphere/AppServer
Node Name	no default	required	Unique node name that cannot contain any of the following special characters / \ * , ; : = + ? < > & % ' " [] # \$ ^ { }. If you plan to federate into an existing cell later, make sure that the name is unique within that cell.
Profile Name	no default	required	A unique profile name. It cannot begin with a period (.) and cannot contain any of the following special characters / \ * , ; : = + ? < > & % ' " [] # \$ ^ { }.
Profile Path	no default	required	Fully qualified path to the stand-alone profile. For example: /opt/IBM/WebSphere/AppServer/profiles/AppServer1
Response File	no default	required	Fully qualified path where the response file that this workflow creates will be located. This file will then be used to drive the installation and profile creation.
Server Name	no default	required	Name of the application server that will be created under the profile.

Additional Input Parameters for Install WebSphere 7 Create Profile

Parameter Name	Default Value	Required	Description
Password	no default	required	The Windows Administrator password. Required for Windows.
Username	no default	required	This is the Windows Administrator user. Required for Windows.

Note: This is the minimum set of parameters required to run this workflow. You may need to expose additional parameters depending on your provisioning objectives.

See ["Parameters for Create StandAlone from Existing WebSphere 7 Install" on page 1285](#) for detailed descriptions of all input parameters for this workflow, including default values.

Tip: To avoid having to re-enter passwords whenever they change, you can create a policy to provide them to the workflow.

3. In the workflow editor, expose any additional parameters that you need. You will specify values for those parameters when you create the deployment.
4. Save the changes to the workflow (click **Save** in the lower right corner).
5. Create a new deployment.
6. On the Parameters tab, specify values for the required parameters listed in step 2 and any additional parameters that you have exposed. You do not need to specify values for those parameters whose default values are appropriate for your environment.
7. On the Targets tab, specify one or more targets for this deployment.
8. Save the deployment (click **Save** in the lower right corner).
9. Run the workflow using this deployment.

To verify the results:

The workflow will complete and report SUCCESS on the Console if it has run successfully. If an error occurs during workflow execution, the error is logged, and the workflow terminates in the FAILURE state.

Optional: if you want to further verify the results, perform the following steps:

1. After the workflow has completed, run the following command to check the version of WebSphere Application Server that was installed:

```
WAS_ROOT/bin/versionInfo.sh
```

Here, *WAS_ROOT* is the directory where WebSphere 7 is installed. This is the path that you specified in the WebSphere Install Location parameter.

2. Validate that stand-alone profile has been created and is running by doing the following:
 - a. View the *WAS_ROOT/profiles/PROFILE_NAME/logs/AboutThisProfile.txt* file. This file is created after the creation of the profile and contains specific information about the profile.

Here, *PROFILE_NAME* is the name of the profile that you just created. This is the name that you specified in the Profile Name parameter.
 - b. Change to the *WAS_ROOT/profiles/PROFILE_NAME/logs/SERVER_NAME* directory, and tail the *SystemOut.log* file. Look for the following line:

```
Server SERVER_NAME open for e-business
```

Here, *SERVER_NAME* is the name of the application server that you just created. This is the name that you specified in the Server Name parameter.

Parameters for Create StandAlone from Existing WebSphere 7 Install

The following tables describe the required and optional input parameters for this workflow. Some of these parameters may not be initially visible in a deployment. For some parameters, if you do not specify a value for a parameter, a default value is assigned.

Parameters Defined in this Step: Validate Existing Install Stand Alone Parameters

Parameter Name	Default Value	Required	Description
Admin Password	no default	optional	When Enable Security is set to true, this parameter must contain a string that does not begin with a dash(-) or contain a space().
Admin User	no default	optional	When Enable Security is set to true, this parameter must contain a string that does not begin with a dash(-), a period (.), or a space(). It cannot contain any of the following characters / \ * , ; ; = + ? < > & % ' " [] # \$ ^ { }.
Cell Name	no default	required	Unique cell name that does not contain any of the following special characters / \ * , ; ; = + ? < > & % ' " [] # \$ ^ { }. If you plan to federate into an existing cell later, make sure that this name is not the same as the existing cell name.
Default Ports	false	optional	Provides the option to assign default ports to a profile. Valid values are true or false. If true, the WebSphere Application Server default ports will be used, and the Ports File and Starting Port parameters should not have values. If false, the workflow will increment the default port until it finds a free port. The default value is false.
Developer Server	no default	optional	Use this parameter for development environments only to help with start up time. Valid value is true. Do not use in production environments.
Enable Security	no default	required	Enables administrative security. Must be set to either true or false. If Enable Security is true, the Admin User and Admin Password parameters must have values.
Host Name	Server.name	required	Hostname or IP address of the target machine.
Install Location	no default	required	Fully qualified path where WebSphere Application Server will be installed. For example: /opt/IBM/WebSphere/AppServer
Keystore Password	no default	optional	Sets the password for all keystore files created during profile creation. This includes keystore files for both the default personal certificate and the root signing certificate.
Node Name	no default	required	Unique node name that cannot contain any of the following special characters / \ * , ; ; = + ? < > & % ' " [] # \$ ^ { }. If you plan to federate into an existing cell later, make sure that the name is unique within that cell.
Omit Action	no default	optional	Enables you to prevent certain optional features from being

Parameters Defined in this Step: Validate Existing Install Stand Alone Parameters, continued

Parameter Name	Default Value	Required	Description
			installed. Valid values are deployAdminConsole or defaultAppDeployAndConfig. You may only specify one of these options.
Personal CertDN	no default	optional	Distinguished name of the personal certificate. For example: CN=dmlab-example.com,OU=WAS7LabCell,OU=WAS7LabDmgrManager,O=IBM,C=US The DN string cannot contain spaces. If you do not specify the DN, the WebSphere Application Server installer will create one.
Personal CertValidity Period	1	optional	Amount of time in years that the personal certificate is valid. Default is one year.
Ports File	no default	optional	Fully qualified path to a file that defines port settings for the new profile. This file must contain key=value pairs that specify a service name and a port number (for example: WC_adminhost=9060). This option should be used with the Validate Ports option.
Profile Name	no default	required	A unique profile name. It cannot begin with a period (.) and cannot contain any of the following special characters / \ * , : ; = + ? < > & % ' " [] # \$ ^ { }.
Profile Path	no default	required	Fully qualified path to the stand-alone profile. For example: /opt/IBM/WebSphere/AppServer/ profiles/AppServer1
Response File	no default	required	Fully qualified path where the response file that this workflow creates will be located. This file will then be used to drive the installation and profile creation.
Server Name	no default	required	Name of the application server that will be created under the profile.
Signing CertDN	no default	optional	Distinguished name of the signing certificate. For example: CN=dmlab-example.com, OU=Root Certificate, OU=WAS7TestLabCell, OU=WAS7LabNode1, O=IBM, C=US The DN string cannot contain spaces. If you do not specify the DN, the WebSphere Application Server installer will create one.
Signing CertValidity Period	15	optional	Amount of time in years that the root certificate is valid. Default is 15 years.
Starting Port	no default	optional	Starting port number that the profile will use to generate and assign port values. Port values are assigned sequentially from the Starting Port. Do not specify this

Parameters Defined in this Step: Validate Existing Install Stand Alone Parameters, continued

Parameter Name	Default Value	Required	Description
			parameter if you specify Default Ports or Ports File.
Validate Ports	no default	optional	Indicates that the ports should be validated to ensure that they are not already in use. Valid values are true or false. You should use this option if you specify a Ports File.
Admin Password	no default	optional	When Enable Security is set to true, this parameter must contain a string that does not begin with a dash(-) or contain a space().

Additional Parameters Defined in this Step: Create WebSphere 7 Profile

Parameter Name	Default Value	Required	Description
Password	no default	required	The Windows Administrator password. Required for Windows.
Username	no default	required	This is the Windows Administrator user. Required for Windows.

Note: Only those parameters that are configurable in a standard deployment are listed here. Input parameters that must be mapped to output parameters of previous steps are not listed.

Create Custom Node from Existing WebSphere 7 Install

Use this workflow to create a custom profile on an existing WebSphere 7 installation.

A custom profile initially contains an empty node with no servers. The workflow can add (federate) the server to the pertinent cell when the profile is created, or you can add it later yourself.

To use this workflow in your environment, see the following information:

Topic	Information Included
"Prerequisites for this Workflow"	List of prerequisites that must be satisfied before you can run this workflow
"How this Workflow Works"	Information about what the workflow does, including validation checks performed, steps executed, and a high-level process flow
"How to Run this Workflow"	Instructions for running this workflow in your environment
"Sample Scenario"	Examples of typical parameter values for this workflow
Parameters	List of input parameters for this workflow

Prerequisites for this Workflow

Be sure that the following prerequisites are satisfied before you run the Create Custom Node from Existing WebSphere 7 Install workflow:

1. This workflow requires unchallenged `sudo` access to a user (typically `root`) who can access all required files and directories.
2. Per the WebSphere 7 documentation, the following system libraries are required before provisioning IBM WebSphere Application Server version 7 on 64-bit Red Hat Linux:

Platform	Required Library
64-bit Red Hat Enterprise Linux version 5	compat-libstdc++-33-3.2.3-61 compat-db-4.2.52-5.1 libXp-1.0.0-8 compat-libstdc++-296-2.96-138 rpm-build-4.4.2-37.el5

Make sure that these libraries exist on each target server before running this workflow. If newer versions of these libraries are available, you can install the newer versions.

3. This workflow will install WebSphere Application Server as `root` because of the following IBM documented limitations:
 - Creation of a Linux service for WebSphere Application Server
 - Native registration with the operating system
 - Port conflicts that may occur with other installations of WebSphere Application Server that are not registered with the operating system

If there is a need to run as a non-root user after installation, you can run a recursive `chown` under the installation root and set owner permissions accordingly.

For more information about prerequisites for WebSphere 7, refer to the [WebSphere 8 Product Documentation](#)

How this Workflow Works

This topic contains the following information about the Create Custom Node from Existing WebSphere 7 Install workflow:

Overview

This workflow does the following things in the order shown:

1. Prepares and validates all parameters and creates the call wrapper that will be used to execute commands within a WebSphere 7 environment
2. Creates a new response file
3. Creates a custom node profile
4. Optionally federates the custom managed node profile into a Deployment Manager

Validation Checks Performed

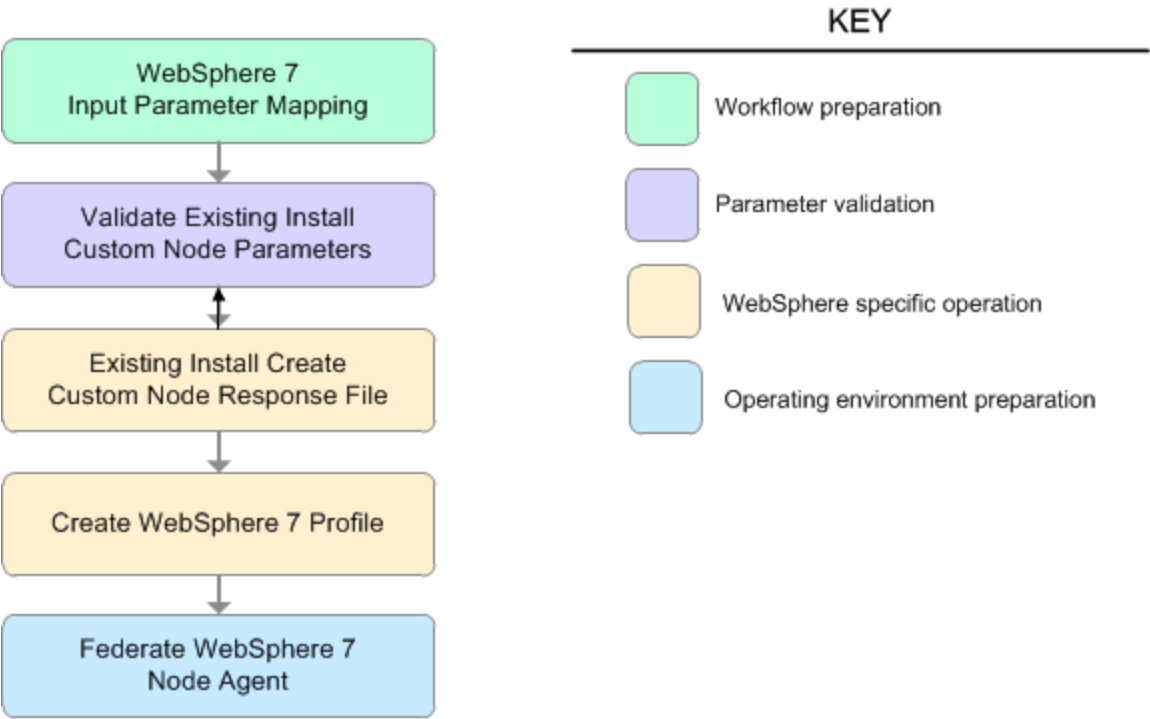
Most of the validation centers on special characters and spaces in the parameters. There are also validation checks that happen at the operating system level, including file system space checks and RPM checks for Red Hat Linux.

The workflow performs the following parameter checks:

1. Enable Security is true or false. If Enable Security is true, Dmgr Admin Password and Dmgr Admin User are specified.
2. Dmgr Admin User (if specified) does not begin with a period (.), hyphen (-) or space. It does not contain any of the following characters: / \ * , : ; = + ? | < > & % ' " [] # \$ ^ { }
3. Dmgr Admin Password (if specified) does not begin with a hyphen (-) or contain a space.
4. Cell Name, Node Name, and Profile Name are specified. They do not contain the following characters: / \ * , : ; = + ? | < > & % ' " [] # \$ ^ { } or space. They do not begin with a period.
5. Host Name is specified.
6. Ports File (if specified) exists.
7. Federate Later (if specified) is true or false.
8. Dmgr Port (if specified) is an integer.
9. Profile Path and Response File are specified.
10. Install Location points to a valid existing WebSphere 7 installation.

Steps Executed

The Create Custom Node from Existing WebSphere 7 Install workflow includes the following steps. Each step must complete successfully before the next step can start. If a step fails, the workflow reports a failure, and all subsequent steps are skipped.



Steps Used in the Create Custom Node from Existing WebSphere 7 Install Workflow

Workflow Step	Description
WebSphere 7 Input Parameter Mapping	This step creates the call wrapper—the command that executes the step as a specific user—and allows certain parameters to be hidden or exposed.
Validate Existing Install Custom Node Parameters	This step prepares and validates the parameters needed to create a custom node profile for an existing WebSphere Application Server V7.0 installation.
Existing Install Create Custom Node Response File	This step creates a new response file to create a custom node profile on top of an existing WebSphere Application Server V7.0 installation.

Steps Used in the Create Custom Node from Existing WebSphere 7 Install Workflow, continued

Workflow Step	Description
Create WebSphere 7 Profile	This step creates a profile on top of an existing WebSphere Application Server V7.0 installation.
Federate WebSphere 7 Node Agent	This step federates the custom managed node profile into a Deployment Manager, creating a node agent.

Sample Scenario

This topic shows you typical parameter values used for the Create Custom Node from Existing WebSphere 7 Install workflow.

Add custom node profiles on existing WebSphere 7 install

Input Parameters for Validate Existing Install Custom Node Parameters

Parameter Name	Example Value	Description
Cell Name	Dev NodeCell	Unique cell name that does not contain any of the following special characters <code>/ \ * , ; = + ? < > & % ' " [] # \$ ^ { }</code> . If you plan to federate into an existing cell later, make sure that this name is not the same as the existing cell name.
Dmgr Admin Password	wasPassWord	Administrative user password for the Deployment Manager. When Enable Security is set to true, this parameter must contain a string that does not begin with a dash(-) or contain a space().
Dmgr Admin User	wasadmin	Deployment Manager administrative user. When Enable Security is set to true, this parameter must contain a string that does not begin with a dash(-), a period(.), or a space(). It cannot contain any of the following characters <code>/ \ * , ; = + ? < > & % ' " [] # \$ ^ { }</code> .
Dmgr HostName	mycompany.com	Host name or IP address of the machine where the Deployment Manager is running. Specify this parameter and the Dmgr Port parameter to federate the new custom node as it is created. If you do not specify a value for this parameter, the new custom node is not federated (you must federate it later). Required if Federate Later is set to false.
Dmgr Port	8879	The SOAP port on which the Deployment Manager is listening. Specify this parameter and the Dmgr Host Name parameter to federate the new custom node as it is created. If you do not specify a value for this parameter, the new custom node is not federated (you must federate it later). Required if Federate Later is set to false.
Enable Security	true	Enables administrative security on the Deployment Manager. Must be set to either true or false. If Enable Security is true, the Dmgr Admin User and Dmgr Admin Password parameters must have values.
Install Location	see description	Fully qualified path where WebSphere Application Server will be installed. For example: <code>/opt/IBM/WebSphere/AppServer</code>
Node Name	DevNode	Unique node name that cannot contain any of the following special characters <code>/ \ * , ; = + ? < > & % ' " [] # \$ ^ { }</code> . If you plan to federate into an existing cell later, make sure that the name is unique within that cell.
Profile Name	DevNode	A unique profile name. It cannot begin with a period (.) and cannot contain any of the following special characters <code>/ \ * , ; = + ? < > & % ' " [] # \$ ^ { }</code> .
Profile Path	see description	Fully qualified path to the custom node profile. For example: <code>/opt/IBM/WebSphere/AppServer/</code>

Input Parameters for Validate Existing Install Custom Node Parameters, continued

Parameter Name	Example Value	Description
		profiles/ProdNode01
Response File	/tmp/serverrsp	Fully qualified path where the response file that this workflow creates will be located. This file will then be used to drive the installation and profile creation.

Tip: To avoid having to re-enter passwords whenever they change, you can create a policy to provide them to the workflow.

How to Run this Workflow

The following instructions show you how to customize and run the Create Custom Node from Existing WebSphere 7 Install workflow in your environment.

The workflow provides default values for some parameters. These default values are usually sufficient for a "typical" installation. You can override the defaults by specifying parameter values in the deployment. You can also expose additional parameters in the workflow, if necessary, to accomplish more advanced scenarios. Any parameters not explicitly specified in the deployment will have the default values listed in ["Parameters for Create Custom Node from Existing WebSphere 7 Install" on page 1300](#)

Note: Before following this procedure, review the ["Prerequisites for this Workflow"](#), and ensure that all requirements are satisfied.

To customize and run the Create Custom Node from Existing WebSphere 7 Install workflow:

1. Create a deployable copy of the workflow.
2. Determine the values that you will specify for the following parameters:

Input Parameters for Validate Existing Install Custom Node Parameters

Parameter Name	Default Value	Required	Description
Cell Name	no default	required	Unique cell name that does not contain any of the following special characters / \ * , ; = + ? < > & % ' " [] # \$ ^ { }. If you plan to federate into an existing cell later, make sure that this name is not the same as the existing cell name.
Dmgr Admin Password	no default	optional	Administrative user password for the Deployment Manager. When Enable Security is set to true, this parameter must contain a string that does not begin with a dash(-) or contain a space().
Dmgr Admin User	no default	optional	Deployment Manager administrative user. When Enable Security is set to true, this parameter must contain a string that does not begin with a dash (-), a period(.), or a space(). It cannot contain any of the following characters / \ * , ; = + ? < > & % ' " [] # \$ ^ { }.
Dmgr HostName	no default	optional	Host name or IP address of the machine where the Deployment

Input Parameters for Validate Existing Install Custom Node Parameters, continued

Parameter Name	Default Value	Required	Description
			Manager is running. Specify this parameter and the Dmgr Port parameter to federate the new custom node as it is created. If you do not specify a value for this parameter, the new custom node is not federated (you must federate it later). Required if Federate Later is set to false.
Dmgr Port	no default	optional	The SOAP port on which the Deployment Manager is listening. Specify this parameter and the Dmgr Host Name parameter to federate the new custom node as it is created. If you do not specify a value for this parameter, the new custom node is not federated (you must federate it later). Required if Federate Later is set to false.
Enable Security	no default	required	Enables administrative security on the Deployment Manager. Must be set to either true or false. If Enable Security is true, the Dmgr Admin User and Dmgr Admin Password parameters must have values.
Install Location	no default	required	Fully qualified path where WebSphere Application Server will be installed. For example: /opt/IBM/WebSphere/AppServer
Node Name	no default	required	Unique node name that cannot contain any of the following special characters / \ * , ; = + ? < > & % ' " [] # \$ ^ { }. If you plan to federate into an existing cell later, make sure that the name is unique within that cell.
Profile Name	no default	required	A unique profile name. It cannot begin with a period (.) and cannot contain any of the following special characters / \ * , ; = + ? < > & % ' " [] # \$ ^ { }.
Profile Path	no default	required	Fully qualified path to the custom node profile. For example: /opt/IBM/WebSphere/AppServer/profiles/ProdNode01
Response File	no default	required	Fully qualified path where the response file that this workflow creates will be located. This file will

Input Parameters for Validate Existing Install Custom Node Parameters, continued

Parameter Name	Default Value	Required	Description
			then be used to drive the installation and profile creation.

Additional Input Parameters for Install WebSphere 7 Create Profile

Parameter Name	Default Value	Required	Description
Password	no default	required	The Windows Administrator password. Required for Windows.
Username	no default	required	This is the Windows Administrator user. Required for Windows.

Note: This is the minimum set of parameters required to run this workflow. You may need to expose additional parameters depending on your provisioning objectives.

See ["Parameters for Create Custom Node from Existing WebSphere 7 Install" on page 1300](#) for detailed descriptions of all input parameters for this workflow, including default values.

Tip: To avoid having to re-enter passwords whenever they change, you can create a policy to provide them to the workflow.

3. In the workflow editor, expose any additional parameters that you need. You will specify values for those parameters when you create the deployment.
4. Save the changes to the workflow (click **Save** in the lower right corner).
5. Create a new deployment.
6. On the Parameters tab, specify values for the required parameters listed in step 2 and any additional parameters that you have exposed. You do not need to specify values for those parameters whose default values are appropriate for your environment.
7. On the Targets tab, specify one or more targets for this deployment.
8. Save the deployment (click **Save** in the lower right corner).
9. Run the workflow using this deployment.

To verify the results:

The workflow will complete and report SUCCESS on the Console if it has run successfully. If an error occurs during workflow execution, the error is logged, and the workflow terminates in the FAILURE state.

Optional: if you want to further verify the results, perform the following steps:

1. After the workflow has completed, run the following command to check the version of WebSphere Application Server that was installed:

```
WAS_ROOT/bin/versionInfo.sh
```

Here, *WAS_ROOT* is the directory where WebSphere 7 is installed. This is the path that you specified in the WebSphere Install Location parameter.

2. Validate that the Deployment Manager profile has been created and is running by doing the following:
 - a. View the *WAS_ROOT/profiles/PROFILE_NAME/logs/AboutThisProfile.txt* file. This file is created after the creation of the profile and contains specific information about the profile.

Here, *PROFILE_NAME* is the name of the profile that you just created. This is the name that you specified in the Profile Name parameter.

- b. Change to the *WAS_ROOT/profiles/PROFILE_NAME/logs/nodeagent* directory, and tail the *SystemOut.log* file. Look for the following line:

```
Server nodeagent open for e-business
```

Parameters for Create Custom Node from Existing WebSphere

7 Install

The following tables describe the required and optional input parameters for this workflow. Some of these parameters may not be initially visible in a deployment. For some parameters, if you do not specify a value for a parameter, a default value is assigned.

Note: Only those parameters that are configurable in a standard deployment are listed here. Input parameters that must be mapped to output parameters of previous steps are not listed.

Parameters Defined in this Step: Validate Existing Install Custom Node Parameters

Parameter Name	Default Value	Required	Description
Cell Name	no default	required	Unique cell name that does not contain any of the following special characters / \ * , ; = + ? < > & % ' " [] # \$ ^ { }. If you plan to federate into an existing cell later, make sure that this name is not the same as the existing cell name.
Dmgr Admin Password	no default	optional	Administrative user password for the Deployment Manager. When Enable Security is set to true, this parameter must contain a string that does not begin with a dash(-) or contain a space().
Dmgr Admin User	no default	optional	Deployment Manager administrative user. When Enable Security is set to true, this parameter must contain a string that does not begin with a dash(-), a period(.), or a space(). It cannot contain any of the following characters / \ * , ; = + ? < > & % ' " [] # \$ ^ { }.
Dmgr HostName	no default	optional	Host name or IP address of the machine where the Deployment Manager is running. Specify this parameter and the Dmgr Port parameter to federate the new custom node as it is created. If you do not specify a value for this parameter, the new custom node is not federated (you must federate it later). Required if Federate Later is set to false.
Dmgr Port	no default	optional	The SOAP port on which the Deployment Manager is listening. Specify this parameter and the Dmgr Host Name parameter to federate the new custom node as it is created. If you do not specify a value for this parameter, the new custom node is not federated (you must federate it later). Required if Federate Later is set to false.
Enable Security	no default	required	Enables administrative security on the Deployment Manager. Must be set to either true or false. If Enable Security is true, the Dmgr Admin User and Dmgr Admin Password parameters must have values.
Host Name	Server.name	required	Hostname or IP address of the target machine.
Install Location	no default	required	Fully qualified path where WebSphere Application Server will be installed. For example: /opt/IBM/WebSphere/AppServer

Parameters Defined in this Step: Validate Existing Install Custom Node Parameters, continued

Parameter Name	Default Value	Required	Description
Keystore Password	no default	optional	Sets the password for all keystore files created during profile creation. This includes keystore files for both the default personal certificate and the root signing certificate.
Node Name	no default	required	Unique node name that cannot contain any of the following special characters <code>/ \ * , : ; = + ? < > & % ' " [] # \$ ^ { }</code> . If you plan to federate into an existing cell later, make sure that the name is unique within that cell.
Personal CertDN	no default	optional	Distinguished name of the personal certificate. For example: CN=dmlab-example.com,OU=WAS7LabCell,OU=WAS7LabDmgrManager,O=IBM,C=US The DN string cannot contain spaces. If you do not specify the DN, the WebSphere Application Server installer will create one.
Personal CertValidity Period	1	optional	Amount of time in years that the personal certificate is valid. Default is one year.
Ports File	no default	optional	Fully qualified path to a file that defines port settings for the new profile. This file must contain key=value pairs that specify a service name and a port number (for example: WC_adminhost=9060). This option should be used with the Validate Ports option.
Profile Name	no default	required	A unique profile name. It cannot begin with a period (.) and cannot contain any of the following special characters <code>/ \ * , : ; = + ? < > & % ' " [] # \$ ^ { }</code> .
Profile Path	no default	required	Fully qualified path to the custom node profile. For example: /opt/IBM/WebSphere/AppServer/ profiles/ProdNode01
Response File	no default	required	Fully qualified path where the response file that this workflow creates will be located. This file will then be used to drive the installation and profile creation.
Signing CertDN	no default	optional	Distinguished name of the signing certificate. For example: CN=dmlab-example.com, OU=Root Certificate, OU=WAS7TestLabCell, OU=WAS7LabNode1, O=IBM, C=US The DN string cannot contain spaces. If you do not specify the DN, the WebSphere Application Server installer will create one.
Signing CertValidity Period	15	optional	Amount of time in years that the root certificate is valid. Default is 15 years.

Additional Parameters Defined in this Step: Install WebSphere 7 Create Profile

Parameter Name	Default Value	Required	Description
Password	no default	required	The Windows Administrator password. Required for Windows.
Username	no default	required	This is the Windows Administrator user. Required for Windows.

Create and Configure WebSphere Data Sources

The purpose of this workflow is to create and configure a new WebSphere Application Server data source within the application server scope. This workflow creates the JDBC (Java Database Connectivity) provider, the J2C (Java 2 Connector) alias, and a data source associated with the JDBC provider.

Data sources—backend connections to an existing database—allow pooling of connections to the database for fast access, reuse by application components, and abstraction of the database connection information by WebSphere.

Supported vendors

The supported database vendors are:

- Oracle Database Enterprise Edition
- Microsoft SQL Server

The following chart shows shows the customizable parameters for WebSphere data sources:

Data source attribute	Configurable parameter
JDBC provider	Database Type (Oracle or SQL Server) Implementation Type (Connection pool source or XA data source) Provider Name Driver Class Path
J2C alias	J2C Alias Name Database User Name Database Password Description
Oracle data source	Oracle URL Java Name Directory Interface (JNDI) Name Data Source Name J2C Alias Name Minimum Pool Connections Maximum Pool Connections
SQL Server data source	Database Name Port Number DB Server Name JNDI Name Data Source Name J2C Alias Name Minimum Pool Connections Maximum Pool Connections

To use this workflow in your environment, see the following information:

Topic	Information Included
"Prerequisites for this Workflow"	List of prerequisites that must be satisfied before you can run this workflow
"How this Workflow Works"	Information about what the workflow does, including validation checks performed, steps executed, and a high-level process flow
"How to Run this Workflow"	Instructions for running this workflow in your environment
"Sample Scenario"	Examples of typical parameter values for this workflow
Parameters	List of input parameters for this workflow

Prerequisites for this Workflow

Be sure that the following prerequisites are satisfied before you run the Create and Configure WebSphere Data Sources workflow.

Product Platform

This workflow is available for WebSphere 7.0, 8.0, or 8.5.x.

Dependencies

This workflow has the following dependencies:

- You must have a working WebSphere Network Deployment cell version 7.0, 8.0, or 8.5.x, with the Deployment Manager available for communication.
- You must run the Discover WebSphere workflow before you run the workflows. The Discover WebSphere workflow audits the server's physical environment for WebSphere cells, clusters, and application servers and stores the configuration information in the DMA environment.
- You need either a working WebSphere Application Server (or servers) or cluster members associated with a cluster.
- You need a running Oracle or SQL Server backend database to connect the data source to.
- A compatible JDBC driver must be on the target machine (or machines). This is available from your database vendor.

For example, a compatible driver for Oracle is `ojdbc6.jar` and for SQL Server is `sqljdbc4.jar`.

For more information about prerequisites for WebSphere, refer to the [WebSphere 8 Product Documentation](#).

How this Workflow Works

The following information describes how the Create and Configure WebSphere Data Sources workflow works:

Overview

This workflow does the following things in the order shown:

1. Before creating the WebSphere data source, the workflow prepares and validates all parameters and creates the call wrapper that will be used to execute commands within a WebSphere environment.
2. Next the workflow stops the WebSphere Application Servers, uses the `AdminTask` command to create the data source according to all the user-specified options, and then restarts the WebSphere Application Servers.
3. Finally, the workflow verifies that the connection to the data source was successful and then discovers the WebSphere configurations associated with the data source.

Validation Checks Performed

The workflow then performs the following checks on the input parameters:

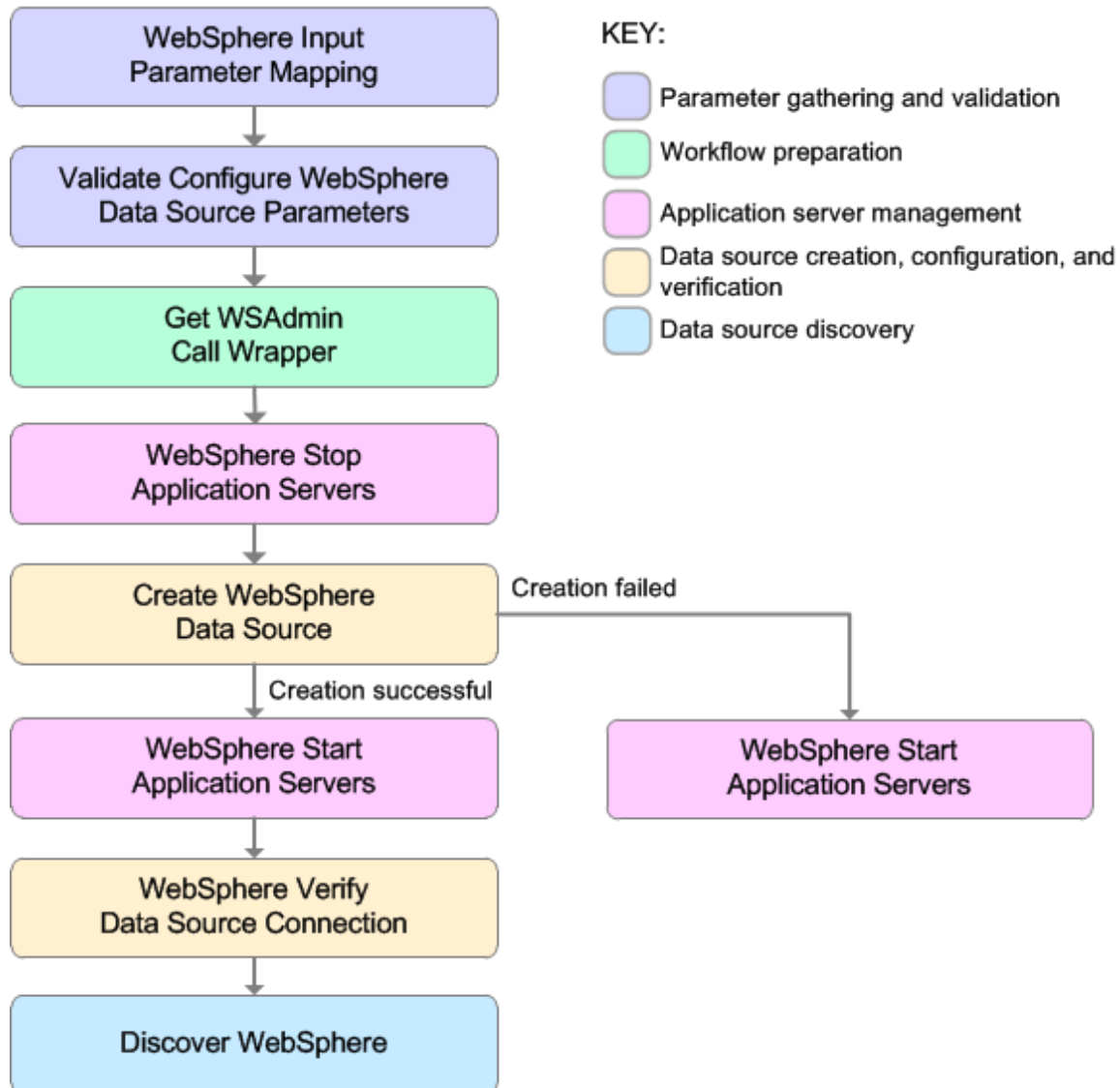
WebSphere Admin Username	Cannot contain the following characters / \ * , : ; = + ? < > & % ' " [] # \$ ^ { } and also cannot begin with a dash (-), period (.), or space ()
WebSphere Admin Password	Cannot begin with a dash (-) and cannot contain a space ()
Enable Security	Must be true or false
If Enable Security is true	WebSphere Admin Username must be specified WebSphere Admin Password must be specified
Database Type	Must be either Oracle or SQL Server (case independent)
Database Type Database Password Database User Name Data Source Name Driver Class Path J2C Alias Name JNDI Name Provider Name	Must be specified
Implementation Type	Must be XA data source or Connection pool data source (case dependent)
If Database Type is Oracle	Oracle URL must be specified Database Name must be null Port Number must be null DB Server Name must be null
If Database Type is SQL Server	Database Name must be specified Port Number must be specified and be numeric DB Server Name must be specified Oracle URL must be null
Maximum Pool Connections Minimum Pool Connections	If specified, must be an integer
Web Service Password Web Service User	Must define a valid WebSphere cluster or application server

The Create and Configure WebSphere Data Sources workflow also checks the environment for the following:

- There needs to be valid organization, server ID, and instance IDs.
- The middleware platform must be WebSphere.
- There must be associated databases.
- The WebSphere container types must be Cluster or APPLICATION_SERVER.

Steps Executed

The Create and Configure WebSphere Data Sources workflow includes the following steps. Each step must complete successfully before the next step can start. If a step fails, the workflow reports a failure and all subsequent steps are skipped.



Steps Used in the Create and Configure WebSphere Data Sources Workflow

Workflow Step	Description
WebSphere Input Parameter Mapping	<p>This step performs the following actions to facilitate the execution of subsequent steps in the workflow:</p> <ol style="list-style-type: none"> 1. Sets the Call Wrapper parameter to its default value. The Call Wrapper is the command that executes a step as a specific user. 2. Allows certain parameters—that may or may not be required depending on what type of action you want to perform—to be hidden or exposed.
Validate Configure WebSphere Data Source Parameters	<p>This step prepares and validates the parameters needed to configure a JDBC provider, J2C alias, and data source for a WebSphere Application Server.</p>
Get WSAAdmin Call Wrapper	<p>This step creates the necessary call wrapper to call <code>wsadmin</code> to execute certain operations within a given WebSphere environment.</p>
WebSphere Stop Application Servers	<p>This step takes a list of WebSphere Application Servers, checks the state of each application server, and stops only the application servers that are in a started state.</p>
Create WebSphere Data Source	<p>This step creates and configures the JDBC provider, J2C alias, and data source within a WebSphere Application Server scope.</p>
WebSphere Start Application Servers	<p>This step takes a list of WebSphere Application Servers, checks the state of each application server, and starts only the application servers that were stopped by the WebSphere Stop Application Servers step.</p>
WebSphere Verify Data Source Connection	<p>This step verifies the connection of a newly created data source within WebSphere.</p>
Discover WebSphere	<p>This step audits the server's physical environment looking for WebSphere cells, clusters, and application servers.</p> <p>Note: Discovery is ONLY additive. It will not remove instances or databases currently in your environment. It is your DMA administrator's responsibility to delete content that is no longer in use.</p>

For parameter descriptions and defaults, see ["Parameters for Create and Configure WebSphere Data Sources"](#) on page 1323.

How to Run this Workflow

The following instructions show you how to customize and run the Create and Configure WebSphere Data Sources workflow in your environment.

The workflow provides default values for some parameters. These default values are usually sufficient for a "typical" installation. You can override the defaults by specifying parameter values in the deployment. You can also expose additional parameters in the workflow, if necessary, to accomplish more advanced scenarios. Any parameters not explicitly specified in the deployment will have the default values listed in ["Parameters for Create and Configure WebSphere Data Sources" on page 1323](#).

Note: Before following this procedure, review the ["Prerequisites for this Workflow"](#), and ensure that all requirements are satisfied.

To use the Create and Configure WebSphere Data Sources workflow:

1. Create a deployable copy of the workflow.
2. Determine the values that you will specify for the following parameters:

Input Parameters for Validate Configure WebSphere Data Source Parameters

Parameter Name	Default Value	Required	Description
Database Name	no default	optional	The name of the SQL Server database. Only used if Database Type is set to SQL Server.
Database Password	no default	required	Password for the database. It will be used for authentication purposes when connecting to the database in order to create the J2C alias.
Database Type	no default	required	The type of database that will be used by the JDBC (Java Database Connectivity) provider. Valid values are Oracle or SQL Server.
Database User Name	no default	required	User name for the database. It will be used for authentication purposes when connecting to the database in order to create the J2C alias.
Data Source Name	no default	required	The name given to the data source when it is created.
DB Server Name	no default	optional	The server name where the database lives. Only used if Database Type is set to SQL Server. For example: dma.mycompany.com
Driver Class Path	no default	required	A list of paths or JAR file names for the resource provider classes. For example: /app/oracle/jdbc/ojdbc6.jar for UNIX and C:\app\oracle\jdbc\ojdbc6.jar for Windows.
Enable	no	required	Indicates whether security will be enabled. Valid

Input Parameters for Validate Configure WebSphere Data Source Parameters , continued

Parameter Name	Default Value	Required	Description
Security	default		values are True or False. If True then WebSphere Admin Password and WebSphere Admin User must have values.
Implementation Type	no default	required	The implementation type for the JDBC (Java Database Connectivity) provider. Use Connection pool data source if your application runs in a single phase or a local transaction. Otherwise, use XA data source to run in a global transaction. Valid values are Connection pool data source or XA data source.
J2C Alias Name	no default	required	Java 2 Connector (J2C) alias name. This will later be used for authentication purposes to map to the data source.
JNDI Name	no default	required	Java Name Directory Interface (JNDI) name. This is a user specified string specific to the application component calls to the data source. For example: jdbc/myDataSource
Oracle URL	no default	optional	Oracle URL for the data source to connect to the database. Only used if Database Type is set to Oracle. For example: jdbc:oracle:thin:@//localhost:1521 for thin or jdbc:oracle:oci:@//localhost:1521 for thick.
Port Number	no default	optional	The port number that the SQL Server database is listening on. Only used if Database Type is set to SQL Server.
Provider Name	no default	required	The name of the JDBC (Java Database Connectivity) provider. For example: My Oracle 11g JDBC Provider.
Trust SSL Certificates	no default	deprecated	DMA no longer uses this workflow parameter to determine whether the workflow will trust any Secure Sockets Layer (SSL) certificate used to connect to the DMA web service. DMA uses the following parameter in the dma.xml file: <Parameter name="com.hp.dma.conn.trustAllCertificates" values="VALUE" /> Here, VALUE is true or false.
Web Service Password	no default	required	Password for the HPE DMA Discovery web service API.
Web Service User	no default	required	A user capable of modifying the HPE DMA managed environment by using the web service API.
WebSphere Admin Password	no default	optional	The password for a user in a group that can change the state of a given application server. Only required if global security is enabled. It cannot not begin with a

Input Parameters for Validate Configure WebSphere Data Source Parameters , continued

Parameter Name	Default Value	Required	Description
			dash (-) or contain a space ().
WebSphere Admin Username	no default	optional	The user account for a user in a group that can change the state of a given application server. Only required if global security is enabled. It cannot begin with a dash (-), a period (.), or a space (). It cannot contain any of the following characters / \ * , ; = + ? < > & % ' " [] # \$ ^ { }.

Tip: To avoid having to re-enter passwords whenever they change, you can create a policy to provide them to the workflow.

Note: This is the minimum set of parameters required to run this workflow. You may need to expose additional parameters depending on your objectives.

See ["Parameters for Create and Configure WebSphere Data Sources" on page 1323](#) for detailed descriptions of all input parameters for this workflow, including default values.

3. In the workflow editor, expose any additional parameters that you need. You will specify values for those parameters when you create the deployment
4. Save the changes to the workflow (click **Save** in the lower right corner).
5. Create a new deployment.
6. On the Parameters tab, specify values for the required parameters listed in step 2 and any additional parameters that you have exposed. You do not need to specify values for those parameters whose default values are appropriate for your environment.
7. On the Targets tab, specify one or more targets for this deployment.
8. Save the deployment (click **Save** in the lower right corner).
9. Run the workflow using this deployment.

To verify the results:

The workflow will complete and report SUCCESS on the Console if it has run successfully. If an error occurs during workflow execution, the error is logged, and the workflow terminates in the FAILURE state.

Optional: If you want to further verify the results:

Use the WebSphere user interface to check that the data source is connected.

Sample Scenario

This topic shows you typical parameter values for different use cases for the Create and Configure WebSphere Data Sources workflow. For a complete list of all parameters used in this workflow, including default values, see ["Parameters for Create and Configure WebSphere Data Sources" on page 1323](#).

The sample scenarios assume that Web Service URL has the value of DMA.URL. This is the default value mapped from the DMA metadata.

Tip: To avoid having to re-enter passwords whenever they change, you can create a policy to provide them to the workflow.

Scenario 1: To create an Oracle data source using connection pool data source

This use case will create an Oracle data source using connection pool data source. This example does not enable security.

Input Parameters for Validate Configure WebSphere Data Source Parameters

Parameter Name	Example Value	Description
Database Password	DbPassWord	Password for the database. It will be used for authentication purposes when connecting to the database in order to create the J2C alias.
Database Type	Oracle	The type of database that will be used by the JDBC (Java Database Connectivity) provider. Valid values are Oracle or SQL Server.
Database User Name	system	User name for the database. It will be used for authentication purposes when connecting to the database in order to create the J2C alias.
Data Source Name	Oracle App Data Source	The name given to the data source when it is created.
Driver Class Path	see description	A list of paths or JAR file names for the resource provider classes. For example: /app/oracle/jdbc/ojdbc6.jar for UNIX and C:\app\oracle\jdbc\ojdbc6.jar for Windows.
Enable Security	False	Indicates whether security will be enabled. Valid values are True or False. If True then WebSphere Admin Password and WebSphere Admin User must have values.
Implementation Type	Connection pool data source	The implementation type for the JDBC (Java Database Connectivity) provider. Use Connection pool data source if your application runs in a single phase or a local transaction. Otherwise, use XA data source to run in a global transaction. Valid values are Connection pool data source or XA data source.
J2C Alias Name	OraAppAlias	Java 2 Connector (J2C) alias name. This will later be used for authentication purposes to map to the data source.

Input Parameters for Validate Configure WebSphere Data Source Parameters , continued

Parameter Name	Example Value	Description
JNDI Name	jdbc/ oraAppDataSource	Java Name Directory Interface (JNDI) name. This is a user specified string specific to the application component calls to the data source. For example: jdbc/myDatasource
Oracle URL	see description	Oracle URL for the data source to connect to the database. Only used if Database Type is set to Oracle. For example: jdbc:oracle:thin:@//localhost:1521 for thin or jdbc:oracle:oci:@//localhost:1521 for thick.
Provider Name	Oracle App JDBC Provider	The name of the JDBC (Java Database Connectivity) provider. For example: My Oracle 11g JDBC Provider.
Web Service Password	myWebSvcPwd	Password for the DMA Discovery web service API.
WebSphere Admin Password	JohnDoe	The password for a user in a group that can change the state of a given application server. Only required if global security is enabled. It cannot not begin with a dash (-) or contain a space ().

Scenario 2: To create an SQL Server data source using connection pool data source

This use case will create an SQL Server data source using connection pool data source and does not enable security.

Input Parameters for Validate Configure WebSphere Data Source Parameters

Parameter Name	Example Value	Description
Database Name	master	The name of the SQL Server database. Only used if Database Type is set to SQL Server.
Database Password	DbPassWord	Password for the database. It will be used for authentication purposes when connecting to the database in order to create the J2C alias.
Database Type	SQL Server	The type of database that will be used by the JDBC (Java Database Connectivity) provider. Valid values are Oracle or SQL Server.
Database User Name	sa	User name for the database. It will be used for authentication purposes when connecting to the database in order to create the J2C alias.
Data Source Name	SQL Server App Data Source	The name given to the data source when it is created.
DB Server Name	see description	The server name where the database lives. Only used if Database Type is set to SQL Server. For example: dma.mycompany.com
Driver Class Path	see description	A list of paths or JAR file names for the resource provider classes. For example: /app/oracle/jdbc/ojdbc6.jar for UNIX and C:\app\oracle\jdbc\ojdbc6.jar for Windows.
Enable Security	False	Indicates whether security will be enabled. Valid values are True or False. If True then WebSphere Admin Password and WebSphere Admin User must have values.
Implementation Type	Connection pool data source	The implementation type for the JDBC (Java Database Connectivity) provider. Use Connection pool data source if your application runs in a single phase or a local transaction. Otherwise, use XA data source to run in a global transaction. Valid values are Connection pool data source or XA data source.
J2C Alias Name	MSSQLAppAlias	Java 2 Connector (J2C) alias name. This will later be used for authentication purposes to map to the data source.
JNDI Name	jdbc/sqlAppDataSource	Java Name Directory Interface (JNDI) name. This is a user specified string specific to the application component calls to the data source. For example: jdbc/myDataSource
Port Number	53074	The port number that the SQL Server database is listening on. Only used if Database Type is set to SQL Server.
Provider Name	MS SQL Server App JDBC Provider	The name of the JDBC (Java Database Connectivity) provider. For example: My Oracle 11g JDBC Provider.

Input Parameters for Validate Configure WebSphere Data Source Parameters , continued

Parameter Name	Example Value	Description
Web Service Password	myWebSvcPwd	Password for the DMA Discovery web service API.
WebSphere Admin Password	JohnDoe	The password for a user in a group that can change the state of a given application server. Only required if global security is enabled. It cannot not begin with a dash (-) or contain a space ().

Scenario 3: To create an Oracle data source using XA data source

This use case will create an Oracle data source using XA data source. To enable security you also need to specify WebSphere Admin Password and WebSphere Admin Username.

Input Parameters for Validate Configure WebSphere Data Source Parameters

Parameter Name	Example Value	Description
Database Password	DbPassWord	Password for the database. It will be used for authentication purposes when connecting to the database in order to create the J2C alias.
Database Type	Oracle	The type of database that will be used by the JDBC (Java Database Connectivity) provider. Valid values are Oracle or SQL Server.
Database User Name	system	User name for the database. It will be used for authentication purposes when connecting to the database in order to create the J2C alias.
Data Source Name	Oracle App XA Data Source	The name given to the data source when it is created.
Driver Class Path	see description	A list of paths or JAR file names for the resource provider classes. For example: /app/oracle/jdbc/ojdbc6.jar for UNIX and C:\app\oracle\jdbc\ojdbc6.jar for Windows.
Enable Security	True	Indicates whether security will be enabled. Valid values are True or False. If True then WebSphere Admin Password and WebSphere Admin User must have values.
Implementation Type	XA data source	The implementation type for the JDBC (Java Database Connectivity) provider. Use Connection pool data source if your application runs in a single phase or a local transaction. Otherwise, use XA data source to run in a global transaction. Valid values are Connection pool data source or XA data source.
J2C Alias Name	OraAppAlias	Java 2 Connector (J2C) alias name. This will later be used for authentication purposes to map to the data source.
JNDI Name	jdbc/oraAppXADataSource	Java Name Directory Interface (JNDI) name. This is a user specified string specific to the application component calls to the data source. For example: jdbc/myDataSource
Oracle URL	see description	Oracle URL for the data source to connect to the database. Only used if Database Type is set to Oracle. For example: jdbc:oracle:thin:@//localhost:1521 for thin or jdbc:oracle:oci:@//localhost:1521 for thick.
Provider Name	Oracle App XA JDBC Provider	The name of the JDBC (Java Database Connectivity) provider. For example: My Oracle 11g JDBC Provider.

Input Parameters for Validate Configure WebSphere Data Source Parameters , continued

Parameter Name	Example Value	Description
Web Service Password	myWebSvcPwd	Password for the DMA Discovery web service API.
Web Service User	JohnDoe	A user capable of modifying the DMA managed environment by using the web service API.
WebSphere Admin Password	myPwd	The password for a user in a group that can change the state of a given application server. Only required if global security is enabled. It cannot not begin with a dash (-) or contain a space ().
WebSphere Admin Username	wasadmin	The user account for a user in a group that can change the state of a given application server. Only required if global security is enabled. It cannot begin with a dash (-), a period (.), or a space (). It cannot contain any of the following characters / \ * , ; = + ? < > & % ' " [] # \$ ^ { }.

Scenario 4: To create an SQL Server data source using XA data source

This use case will create an SQL Server data source using XA data source and specifying the Maximum and Minimum Pool Connections. This example does not enable security.

Note: Some of these parameters are not exposed by default in the deployment. You need to expose the following in the step Validate Configure WebSphere Data Source Parameters:

- Maximum Pool Connections
- Minimum Pool Connections

Input Parameters for Validate Configure WebSphere Data Source Parameters

Parameter Name	Example Value	Description
Database Name	master	The name of the SQL Server database. Only used if Database Type is set to SQL Server.
Database Password	DbPassWord	Password for the database. It will be used for authentication purposes when connecting to the database in order to create the J2C alias.
Database Type	SQL Server	The type of database that will be used by the JDBC (Java Database Connectivity) provider. Valid values are Oracle or SQL Server.
Database User Name	sa	User name for the database. It will be used for authentication purposes when connecting to the database in order to create the J2C alias.
Data Source Name	SQL Server App XA Data Source	The name given to the data source when it is created.
DB Server Name	see description	The server name where the database lives. Only used if Database Type is set to SQL Server. For example: dma.mycompany.com
Driver Class Path	see description	A list of paths or JAR file names for the resource provider classes. For example: /app/oracle/jdbc/ojdbc6.jar for UNIX and C:\app\oracle\jdbc\ojdbc6.jar for Windows.
Enable Security	False	Indicates whether security will be enabled. Valid values are True or False. If True then WebSphere Admin Password and WebSphere Admin User must have values.
Implementation Type	XA data source	The implementation type for the JDBC (Java Database Connectivity) provider. Use Connection pool data source if your application runs in a single phase or a local transaction. Otherwise, use XA data source to run in a global transaction. Valid values are Connection pool data source or XA data source.
J2C Alias Name	MSSQLAppAlias	Java 2 Connector (J2C) alias name. This will later be used for authentication purposes to map to the data

Input Parameters for Validate Configure WebSphere Data Source Parameters, continued

Parameter Name	Example Value	Description
		source.
JNDI Name	jdbc/ sqlAppXADataSource	Java Name Directory Interface (JNDI) name. This is a user specified string specific to the application component calls to the data source. For example: jdbc/myDatasource
Maximum Pool Connections	40	The maximum number of connections to be maintained in the data source connection pool. The default is the WebSphere default value.
Minimum Pool Connections	20	The minimum number of connections to be maintained in the data source connection pool. The default is the WebSphere default value.
Port Number	53074	The port number that the SQL Server database is listening on. Only used if Database Type is set to SQL Server.
Provider Name	MS SQL Server App XA JDBC Provider	The name of the JDBC (Java Database Connectivity) provider. For example: My Oracle 11g JDBC Provider.
Web Service Password	myWebSvcPwd	Password for the DMA Discovery web service API.
Web Service User	JohnDoe	A user capable of modifying the DMA managed environment by using the web service API.

Parameters for Create and Configure WebSphere Data Sources

The following tables describe the required and optional input parameters for this workflow. Most of these parameters are not initially visible in a deployment. For most parameters, if you do not specify a value for a parameter, a default value is assigned.

Parameters Defined in this Step: Validate Configure WebSphere Data Source Parameters

Parameter Name	Default Value	Required	Description
Database Name	no default	optional	The name of the SQL Server database. Only used if Database Type is set to SQL Server.
Database Password	no default	required	Password for the database. It will be used for authentication purposes when connecting to the database in order to create the J2C alias.
Database Type	no default	required	The type of database that will be used by the JDBC (Java Database Connectivity) provider. Valid values are Oracle or SQL Server.
Database User Name	no default	required	User name for the database. It will be used for authentication purposes when connecting to the database in order to create the J2C alias.
Data Source Name	no default	required	The name given to the data source when it is created.
DB Server Name	no default	optional	The server name where the database lives. Only used if Database Type is set to SQL Server. For example: dma.mycompany.com
Driver Class Path	no default	required	A list of paths or JAR file names for the resource provider classes. For example: /app/oracle/jdbc/ojdbc6.jar for UNIX and C:\app\oracle\jdbc\ojdbc6.jar for Windows.
Enable Security	no default	required	Indicates whether security will be enabled. Valid values are True or False. If True then WebSphere Admin Password and WebSphere Admin User must have values.
Implementation Type	no default	required	The implementation type for the JDBC (Java Database Connectivity) provider. Use Connection pool data source if your application runs in a single phase or a local transaction. Otherwise, use XA data source to run in a global transaction. Valid values are Connection pool data source or XA data source.
J2C Alias Name	no default	required	Java 2 Connector (J2C) alias name. This will later be used for authentication purposes to map to the data source.
JNDI Name	no default	required	Java Name Directory Interface (JNDI) name. This is a user specified string specific to the application component calls to the data source. For example: jdbc/myDatasource

Parameters Defined in this Step: Validate Configure WebSphere Data Source Parameters , continued

Parameter Name	Default Value	Required	Description
Maximum Pool Connections	see description	optional	The maximum number of connections to be maintained in the data source connection pool. The default is the WebSphere default value.
Minimum Pool Connections	see description	optional	The minimum number of connections to be maintained in the data source connection pool. The default is the WebSphere default value.
Oracle URL	no default	optional	Oracle URL for the data source to connect to the database. Only used if Database Type is set to Oracle. For example: jdbc:oracle:thin:@//localhost:1521 for thin or jdbc:oracle:oci:@//localhost:1521 for thick.
Port Number	no default	optional	The port number that the SQL Server database is listening on. Only used if Database Type is set to SQL Server.
Provider Name	no default	required	The name of the JDBC (Java Database Connectivity) provider. For example: My Oracle 11g JDBC Provider.
Provider Type	no default	required	The JDBC (Java Database Connectivity) provider type. Valid values are Oracle JDBC Driver or Microsoft SQL Server JDBC Driver.
Trust SSL Certificates	no default	deprecated	DMA no longer uses this workflow parameter to determine whether the workflow will trust any Secure Sockets Layer (SSL) certificate used to connect to the DMA web service. DMA uses the following parameter in the dma.xml file: <Parameter name="com.hp.dma.conn.trustAllCertificates" values="VALUE" /> Here, VALUE is true or false.
Web Service Password	no default	required	Password for the DMA Discovery web service API.
Web Service User	no default	required	A user capable of modifying the DMA managed environment by using the web service API.
WebSphere Admin Password	no default	optional	The password for a user in a group that can change the state of a given application server. Only required if global security is enabled. It cannot not begin with a dash (-) or contain a space ().
WebSphere Admin Username	no default	optional	The user account for a user in a group that can change the state of a given application server. Only required if global security is enabled. It cannot begin with a dash (-), a period (.), or a space (). It cannot contain any of the following characters / \ * , ; = + ? < > & % ' " [] # \$ ^ { }.

Create and Configure WebSphere Web Server Definitions

The purpose of this workflow is to configure web server objects in a given WebSphere Application Server cell. These web server objects can be used later when deploying applications into a given application server or cluster. They also give limited ability to administer the web server instances.

First, the workflow creates an unmanaged node that represents the system where the web servers are running. Second, the workflow creates the web server definition under the unmanaged node. This node will hold information about the web server instance that runs on either the same machine or a remote machine.

Context

After the web server has been created an application can be installed and mapped to these web server objects at deployment time. Then a plug-in component can be generated based on the application configuration and application server information. The workflow consolidates that information into a single xml file that will be read by the web server plug-in.

Supported vendor

The supported web server vendor is IBM HTTP Server.

To use this workflow in your environment, see the following information:

Topic	Information Included
"Prerequisites for this Workflow"	List of prerequisites that must be satisfied before you can run this workflow
"How this Workflow Works"	Information about what the workflow does, including validation checks performed, steps executed, and a high-level process flow
"How to Run this Workflow"	Instructions for running this workflow in your environment
"Sample Scenario"	Examples of typical parameter values for this workflow
Parameters	List of input parameters for this workflow

Prerequisites for this Workflow

Be sure that the following prerequisites are satisfied before you run the Create and Configure WebSphere Web Server Definitions workflow.

Product Platform

This workflow is available for WebSphere 7.0, 8.0, or 8.5.x.

Dependencies

This workflow has the following dependencies:

- You must have a working WebSphere Network Deployment cell version 7.0, 8.0, or 8.5.x, with the Deployment Manager available for communication.
- You must run the Discover WebSphere workflow before you run the workflows. The Discover WebSphere workflow audits the server's physical environment for WebSphere cells, clusters, and application servers and stores the configuration information in the DMA environment.

For more information about prerequisites for WebSphere, refer to the [WebSphere 8 Product Documentation](#).

How this Workflow Works

The following information describes how the Create and Configure WebSphere Web Server Definitions workflow works:

Overview

This workflow does the following things in the order shown:

1. Before creating the WebSphere web server definitions, the workflow prepares and validates all parameters and creates the call wrapper that will be used to execute commands within a WebSphere environment .
2. Next the workflow uses the AdminTask command with all the user-specified options to create and configure the WebSphere unmanaged node and to create an IHS web server definition. Then the workflow synchronizes the node if it is enabled.
3. Finally, the workflow discovers the web server definitions associated with a WebSphere node.

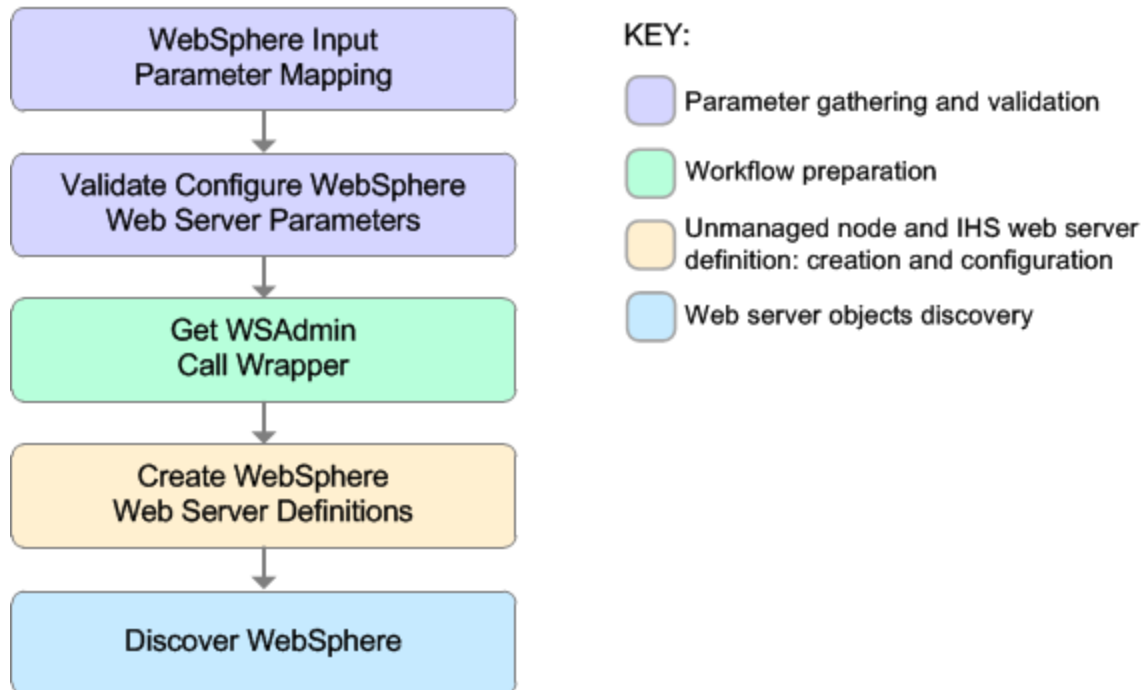
Validation Checks Performed

The workflow then performs the following checks on the input parameters:

Access Log File Error Log File HTTP Configuration File Plugin Install Root Web Server Install Root	Must be specified
Admin Protocol HTTP Web Protocol	If not specified, set to HTTP If specified, must be HTTP or HTTPS (case independent)
Unmanaged Node Host Name Unmanaged Node Name Web Server Name	Must be specified Cannot contain the following characters / \ * , : ; = + ? < > & % ' " [] # \$ ^ { } or space Cannot begin with a period (.)
HTTP Admin Password	Cannot begin with a dash (-) and cannot contain a space ()
HTTP Admin User	Cannot contain the following characters / \ * , : ; = + ? < > & % ' " [] # \$ ^ { } and also cannot begin with a dash (-), period (.), or space ()
HTTP Admin Port HTTP Web Port	Must be specified Must be an integer
Node Operating System	Must be aix, linux, solaris, or windows (case independent)
WebApp Mapping	If not specified, set to NONE If specified, must be ALL or NONE (case independent)
WebSphere Admin Username	Cannot contain the following characters / \ * , : ; = + ? < > & % ' " [] # \$ ^ { } and also cannot begin with a dash (-), period (.), or space ()
WebSphere Admin Password	Cannot begin with a dash (-) and cannot contain a space ()
Enable Security	Must be true or false
If Enable Security is true	WebSphere Admin Username must be specified WebSphere Admin Password must be specified
Web Service Password Web Service User	Must define a valid WebSphere Home

Steps Executed

The Create and Configure WebSphere Web Server Definitions workflow includes the following steps. Each step must complete successfully before the next step can start. If a step fails, the workflow reports a failure and all subsequent steps are skipped.



Steps Used in the Create and Configure WebSphere Web Server Definitions Workflow

Workflow Step	Description
WebSphere Input Parameter Mapping	<p>This step performs the following actions to facilitate the execution of subsequent steps in the workflow:</p> <ol style="list-style-type: none"> 1. Sets the Call Wrapper parameter to its default value. The Call Wrapper is the command that executes a step as a specific user. 2. Allows certain parameters—that may or may not be required depending on what type of action you want to perform—to be hidden or exposed.
Validate Configure WebSphere Web Server Parameters	<p>This step prepares and validates the parameters needed to create and configure an unmanaged node and create an IHS web server definition.</p>
Get WSAAdmin Call Wrapper	<p>This step creates the necessary call wrapper to call <code>wsadmin</code> to execute certain operations within a given WebSphere environment.</p>
Create WebSphere Web Server Definitions	<p>This step creates and configures the WebSphere unmanaged node and IHS web server definition.</p>
Discover WebSphere	<p>This step audits the server's physical environment looking for WebSphere cells, clusters, and application servers.</p> <p>Note: Discovery is ONLY additive. It will not remove instances or databases currently in your environment. It is your DMA administrator's responsibility to delete content that is no longer in use.</p>

For parameter descriptions and defaults, see ["Parameters for Create and Configure WebSphere Web Server Definitions" on page 1338](#).

How to Run this Workflow

The following instructions show you how to customize and run the Create and Configure WebSphere Web Server Definitions workflow in your environment.

The workflow provides default values for some parameters. These default values are usually sufficient for a "typical" installation. You can override the defaults by specifying parameter values in the deployment.

Note: Before following this procedure, review the ["Prerequisites for this Workflow"](#), and ensure that all requirements are satisfied.

To use the Create and Configure WebSphere Web Server Definitions workflow:

1. Create a deployable copy of the workflow.
2. Determine the values that you will specify for the following parameters:

Input Parameters for Validate Configure WebSphere Web Server Parameters

Parameter Name	Default Value	Required	Description
Access Log File	no default	required	Fully qualified path for the IBM HTTP Server access log file. For example: /opt/IBM/HTTPServer/logs/access.log
Admin Protocol	HTTP	optional	Administrative protocol title. Valid values are HTTP or HTTPS. The default is HTTP.
Enable Security	no default	required	Indicates whether security will be enabled. Valid values are True or False. If True then WebSphere Admin Password and WebSphere Admin User must have values.
Error Log File	no default	required	Fully qualified path for the IBM HTTP Server error log file. For example: /opt/IBM/HTTPServer/logs/error.log
HTTP Admin Password	no default	optional	Password for the HTTP Admin User.
HTTP Admin Port	8008	required	Port of the IBM HTTP Server administrative server.
HTTP Admin User	no default	optional	User name of the IBM HTTP administrative user.
HTTP Configuration File	no default	required	Fully qualified path for the IBM HTTP Server configuration file. For example: /opt/IBM/HTTPServer/conf/httpd.conf
HTTP Web Port	80	required	Port number of the IBM HTTP web server.

Input Parameters for Validate Configure WebSphere Web Server Parameters, continued

Parameter Name	Default Value	Required	Description
HTTP Web Protocol	HTTP	required	The protocol used by the IBM HTTP Server administrative server running with an unmanaged or remote web server. Valid values are HTTP or HTTPS. The default is HTTP.
Node Operating System	no default	required	The operating system in use on the system associated with the node specified in Unmanaged Node Name. Valid values are: aix, linux, solaris, windows.
Plugin Install Root	no default	required	The installation root directory where the plug-in for the web server is installed. For example: /opt/IBM/HTTPServer/Plugin
Service Name	no default	optional	The Windows service name for the IBM HTTP Server. Only required if the Node Operating System is Windows.
Trust SSL Certificates	no default	deprecated	DMA no longer uses this workflow parameter to determine whether the workflow will trust any Secure Sockets Layer (SSL) certificate used to connect to the DMA web service. DMA uses the following parameter in the dma.xml file: <pre><Parameter name="com.hp.dma.conn.trustAllCertificates" values="VALUE" /></pre> Here, VALUE is true or false.
Unmanaged Node Host Name	no default	required	Host name of the system associated with the node specified in Unmanaged Node Name.
Unmanaged Node Name	no default	required	The node name in the configuration repository.
WebApp Mapping	NONE	optional	Level of installed web applications mapped to the web server. Valid values are ALL or NONE. The default is NONE.
Web Server Install Root	no default	required	Fully qualified directory path for the web server. For example: /opt/IBM/HTTPServer
Web Server Name	no default	required	Name of the IBM HTTP web server.
Web Service Password	no default	required	Password for the DMA Discovery web service API.
Web Service User	no default	required	A user capable of modifying the DMA managed environment by using the web service API.
WebSphere	no default	optional	The password for a user in a group that can

Input Parameters for Validate Configure WebSphere Web Server Parameters, continued

Parameter Name	Default Value	Required	Description
Admin Password			change the state of a given application server. Only required if global security is enabled. It cannot not begin with a dash (-) or contain a space ().
WebSphere Admin Username	no default	optional	The user account for a user in a group that can change the state of a given application server. Only required if global security is enabled. It cannot begin with a dash (-), a period (.), or a space (). It cannot contain any of the following characters / \ * , ; = + ? < > & % ' " [] # \$ ^ { }.

Tip: To avoid having to re-enter passwords whenever they change, you can create a policy to provide them to the workflow.

Note: See ["Parameters for Create and Configure WebSphere Web Server Definitions" on page 1338](#) for detailed descriptions of all input parameters for this workflow, including default values.

3. In the workflow editor, expose any additional parameters that you need. You will specify values for those parameters when you create the deployment
4. Save the changes to the workflow (click **Save** in the lower right corner).
5. Create a new deployment.
6. On the Parameters tab, specify values for the required parameters listed in step 2 and any additional parameters that you have exposed. You do not need to specify values for those parameters whose default values are appropriate for your environment.
7. On the Targets tab, specify one or more targets for this deployment.
8. Save the deployment (click **Save** in the lower right corner).
9. Run the workflow using this deployment.

To verify the results:

The workflow will complete and report SUCCESS on the Console if it has run successfully. If an error occurs during workflow execution, the error is logged, and the workflow terminates in the FAILURE state.

Optional: If you want to further verify the results:

Use the WebSphere administrative console interface to check that the web server is configured.

Sample Scenario

This topic shows you typical parameter values for different use cases for the Create and Configure WebSphere Web Server Definitions workflow. For a complete list of all parameters used in this workflow, including default values, see ["Parameters for Create and Configure WebSphere Web Server Definitions" on page 1338](#).

Tip: To avoid having to re-enter passwords whenever they change, you can create a policy to provide them to the workflow.

Scenario 1: To create and configure a WebSphere unmanaged node and web server definitions using unsecured protocol

This use case will create and configure a WebSphere unmanaged node and web server definitions using unsecured protocol. This example also does the following:

- Does not enable security
- Has the Linux operating system on the node
- Does not map any web applications to the web server

Input Parameters for Validate Configure WebSphere Web Server Parameters

Parameter Name	Example Value	Description
Access Log File	see description	Fully qualified path for the IBM HTTP Server access log file. For example: /opt/IBM/HTTPServer/logs/access.log
Admin Protocol	HTTP	Administrative protocol title. Valid values are HTTP or HTTPS. The default is HTTP.
Enable Security	False	Indicates whether security will be enabled. Valid values are True or False. If True then WebSphere Admin Password and WebSphere Admin User must have values.
Error Log File	see description	Fully qualified path for the IBM HTTP Server error log file. For example: /opt/IBM/HTTPServer/logs/error.log
HTTP Admin Password	HttpPassWoRd	Password for the HTTP Admin User.
HTTP Admin Port	8008	Port of the IBM HTTP Server administrative server.
HTTP Admin User	httpadmin	User name of the IBM HTTP administrative user.
HTTP Configuration File	see description	Fully qualified path for the IBM HTTP Server configuration file. For example: /opt/IBM/HTTPServer/conf/httpd.conf
HTTP Web Port	80	Port number of the IBM HTTP web server.

Input Parameters for Validate Configure WebSphere Web Server Parameters, continued

Parameter Name	Example Value	Description
HTTP Web Protocol	HTTP	The protocol used by the IBM HTTP Server administrative server running with an unmanaged or remote web server. Valid values are HTTP or HTTPS. The default is HTTP.
Node Operating System	linux	The operating system in use on the system associated with the node specified in Unmanaged Node Name. Valid values are: aix, linux, solaris, windows.
Plugin Install Root	see description	The installation root directory where the plug-in for the web server is installed. For example: /opt/IBM/HTTPServer/Plugin
Unmanaged Node Host Name	see description	Host name of the system associated with the node specified in Unmanaged Node Name. For example: example.mycompany.com
Unmanaged Node Name	webServerNode	The node name in the configuration repository.
WebApp Mapping	NONE	Level of installed web applications mapped to the web server. Valid values are ALL or NONE. The default is NONE.
Web Server Install Root	see description	Fully qualified directory path for the web server. For example: /opt/IBM/HTTPServer
Web Server Name	WebServer1	Name of the IBM HTTP web server.
Web Service Password	myWebSvcPwd	Password for the DMA Discovery web service API.
Web Service User	JohnDoe	A user capable of modifying the DMA managed environment by using the web service API.

Scenario 2: To create and configure a WebSphere unmanaged node and web server definitions using secured protocol

This use case will create and configure a WebSphere unmanaged node and web server definitions using unsecured protocol. This example also does the following:

- Enables security—WebSphere Admin Password and WebSphere Admin Username also need to be provided
- Has the AIX operating system on the node
- Maps all web applications to the web server

Input Parameters for Validate Configure WebSphere Web Server Parameters

Parameter Name	Example Value	Description
Access Log File	see description	Fully qualified path for the IBM HTTP Server access log file. For example: <code>/opt/IBM/HTTPServer/logs/access.log</code>
Admin Protocol	HTTPS	Administrative protocol title. Valid values are HTTP or HTTPS. The default is HTTP.
Enable Security	True	Indicates whether security will be enabled. Valid values are True or False. If True then WebSphere Admin Password and WebSphere Admin User must have values.
Error Log File	see description	Fully qualified path for the IBM HTTP Server error log file. For example: <code>/opt/IBM/HTTPServer/logs/error.log</code>
HTTP Admin Password	HttpPassWoRd	Password for the HTTP Admin User.
HTTP Admin Port	8443	Port of the IBM HTTP Server administrative server.
HTTP Admin User	htpadmin	User name of the IBM HTTP administrative user.
HTTP Configuration File	see description	Fully qualified path for the IBM HTTP Server configuration file. For example: <code>/opt/IBM/HTTPServer/conf/httpd.conf</code>
HTTP Web Port	443	Port number of the IBM HTTP web server.
HTTP Web Protocol	HTTPS	The protocol used by the IBM HTTP Server administrative server running with an unmanaged or remote web server. Valid values are HTTP or HTTPS. The default is HTTP.
Node Operating System	aix	The operating system in use on the system associated with the node specified in Unmanaged Node Name. Valid values are: aix, linux, solaris, windows.
Plugin Install Root	see description	The installation root directory where the plug-in for the web server is installed. For example: <code>/opt/IBM/HTTPServer/Plugin</code>
Unmanaged	see description	Host name of the system associated with the node specified in

Input Parameters for Validate Configure WebSphere Web Server Parameters, continued

Parameter Name	Example Value	Description
Node Host Name		Unmanaged Node Name. For example: <code>example.mycompany.com</code>
Unmanaged Node Name	<code>webServerNode</code>	The node name in the configuration repository.
WebApp Mapping	<code>ALL</code>	Level of installed web applications mapped to the web server. Valid values are <code>ALL</code> or <code>NONE</code> . The default is <code>NONE</code> .
Web Server Install Root	see description	Fully qualified directory path for the web server. For example: <code>/opt/IBM/HTTPServer</code>
Web Server Name	<code>WebServer1</code>	Name of the IBM HTTP web server.
Web Service Password	<code>myWebSvcPwd</code>	Password for the DMA Discovery web service API.
Web Service User	<code>JohnDoe</code>	A user capable of modifying the DMA managed environment by using the web service API.
WebSphere Admin Password	<code>myPwd</code>	The password for a user in a group that can change the state of a given application server. Only required if global security is enabled. It cannot not begin with a dash (-) or contain a space ().
WebSphere Admin Username	<code>wasadmin</code>	The user account for a user in a group that can change the state of a given application server. Only required if global security is enabled. It cannot begin with a dash (-), a period (.), or a space (). It cannot contain any of the following characters <code>/ \ * , ; ; = + ? < > & % ' " [] # \$ ^ { }</code> .

Parameters for Create and Configure WebSphere Web Server Definitions

The following tables describe the required and optional input parameters for this workflow. For most parameters, if you do not specify a value for a parameter, a default value is assigned.

Parameters Defined in this Step: Validate Configure WebSphere Web Server Parameters

Parameter Name	Default Value	Required	Description
Access Log File	no default	required	Fully qualified path for the IBM HTTP Server access log file. For example: <code>/opt/IBM/HTTPServer/logs/access.log</code>
Admin Protocol	HTTP	optional	Administrative protocol title. Valid values are HTTP or HTTPS. The default is HTTP.
Enable Security	no default	required	Indicates whether security will be enabled. Valid values are True or False. If True then WebSphere Admin Password and WebSphere Admin User must have values.
Error Log File	no default	required	Fully qualified path for the IBM HTTP Server error log file. For example: <code>/opt/IBM/HTTPServer/logs/error.log</code>
HTTP Admin Password	no default	optional	Password for the HTTP Admin User.
HTTP Admin Port	8008	required	Port of the IBM HTTP Server administrative server.
HTTP Admin User	no default	optional	User name of the IBM HTTP administrative user.
HTTP Configuration File	no default	required	Fully qualified path for the IBM HTTP Server configuration file. For example: <code>/opt/IBM/HTTPServer/conf/httpd.conf</code>
HTTP Web Port	80	required	Port number of the IBM HTTP web server.
HTTP Web Protocol	HTTP	required	The protocol used by the IBM HTTP Server administrative server running with an unmanaged or remote web server. Valid values are HTTP or HTTPS. The default is HTTP.
Node Operating System	no default	required	The operating system in use on the system associated with the node specified in Unmanaged Node Name. Valid values are: aix, linux, solaris, windows.
Plugin Install Root	no default	required	The installation root directory where the plug-in for the web server is installed. For example: <code>/opt/IBM/HTTPServer/Plugin</code>
Service Name	no default	optional	The Windows service name for the IBM HTTP Server. Only required if the Node Operating System is Windows.
Trust SSL Certificates	no default	deprecated	DMA no longer uses this workflow parameter to determine whether the workflow will trust any Secure Sockets Layer (SSL) certificate used to connect to the DMA web service. DMA uses the following parameter in the <code>dma.xml</code> file:

Parameters Defined in this Step: Validate Configure WebSphere Web Server Parameters, continued

Parameter Name	Default Value	Required	Description
			<pre><Parameter name="com.hp.dma.conn.trustAllCertificates" values="VALUE" /></pre> <p>Here, VALUE is true or false.</p>
Unmanaged Node Host Name	no default	required	Host name of the system associated with the node specified in Unmanaged Node Name.
Unmanaged Node Name	no default	required	The node name in the configuration repository.
WebApp Mapping	NONE	optional	Level of installed web applications mapped to the web server. Valid values are ALL or NONE. The default is NONE.
Web Server Install Root	no default	required	Fully qualified directory path for the web server. For example: /opt/IBM/HTTPServer
Web Server Name	no default	required	Name of the IBM HTTP web server.
Web Service Password	no default	required	Password for the DMA Discovery web service API.
Web Service User	no default	required	A user capable of modifying the DMA managed environment by using the web service API.
WebSphere Admin Password	no default	optional	The password for a user in a group that can change the state of a given application server. Only required if global security is enabled. It cannot not begin with a dash (-) or contain a space ().
WebSphere Admin Username	no default	optional	The user account for a user in a group that can change the state of a given application server. Only required if global security is enabled. It cannot begin with a dash (-), a period (.), or a space (). It cannot contain any of the following characters / \ * , ; : = + ? < > & % ' " [] # \$ ^ { }.

WebSphere - Code Release

This workflow automates application deployments in IBM WebSphere. In addition to deployment automation, this workflow can update JVM Generic Arguments and JVM System Properties on the Web Server, and also provides install options for application deployments.

Some install options are provided as parameters for the workflow, or, users can specify install options within a file for each of the applications to be deployed (Note that user-specified parameter values take the highest precedence). This workflow provides application deployment verification by providing the URLs. For successful application deployments, verifications and a list of the applications are

maintained in the history file. In cases of unsuccessful application deployments, the workflow rolls back the deployment and restores the last successfully deployed application (if any).

The supported applications are of type :

- .war files
- .ear files

To use this workflow in your environment, see the following information:

Topic	Information Included
"Prerequisites for this Workflow"	List of prerequisites that must be satisfied before you can run this workflow
"How this Workflow Works"	Information about what the workflow does, including validation checks performed, steps executed, and a high-level process flow
"How to Run this Workflow"	Instructions for running this workflow in your environment
"Sample Scenario"	Examples of typical parameter values for this workflow
"Parameters for WebSphere - Code Release" on page 1355	List of input parameters for this workflow

Prerequisites for this Workflow

Be sure that the following prerequisites are satisfied before you run the WebSphere - Code Release workflow.

Product Platform

This workflow is available for WebSphere7.0, 8.0, or 8.5.x.

Dependencies

This workflow has the following dependencies:

- You must have a working WebSphere Network Deployment cell version 7.0, 8.0, or 8.5.x, with the Deployment Manager available for communication.
- You must run the Discover WebSphere workflow before you run the workflows. The Discover WebSphere workflow audits the server's physical environment for WebSphere cells, clusters, and application servers and stores the configuration information in the DMA environment.

For more information about prerequisites for WebSphere, refer to the [WebSphere 8 Product Documentation](#).

How this Workflow Works

The following information describes how the WebSphere - Code Release workflow works:

Overview

This workflow does the following things in the order shown:

1. Initially, the workflow inputs all parameters, set defaults for optional parameters, and validates all parameters. If input files do not exist in the specified locations, they are downloaded from the software repository. The workflow performs a checksum to verify that the archive files should be deployed in the Application Server on a standalone setup.
2. Next, the workflow creates the installation options and the call wrapper that will be used to execute commands within a WebSphere environment. The workflow updates the JVM setting and then creates a backup. The workflow deploys the specified Application Archive files in the Application Server on a standalone setup.
3. If the application deployment succeeds, the workflow tests the URLs for the web servers and copies the application archives.
4. If the application deployment fails, the workflow rolls back the deployment and restores the last successfully deployed application (if any).
5. Finally, the workflow cleans up downloaded files based on the Cleanup on Success and Cleanup on Failure parameters.

Validation Checks Performed

The workflow performs the following checks on the input parameters:

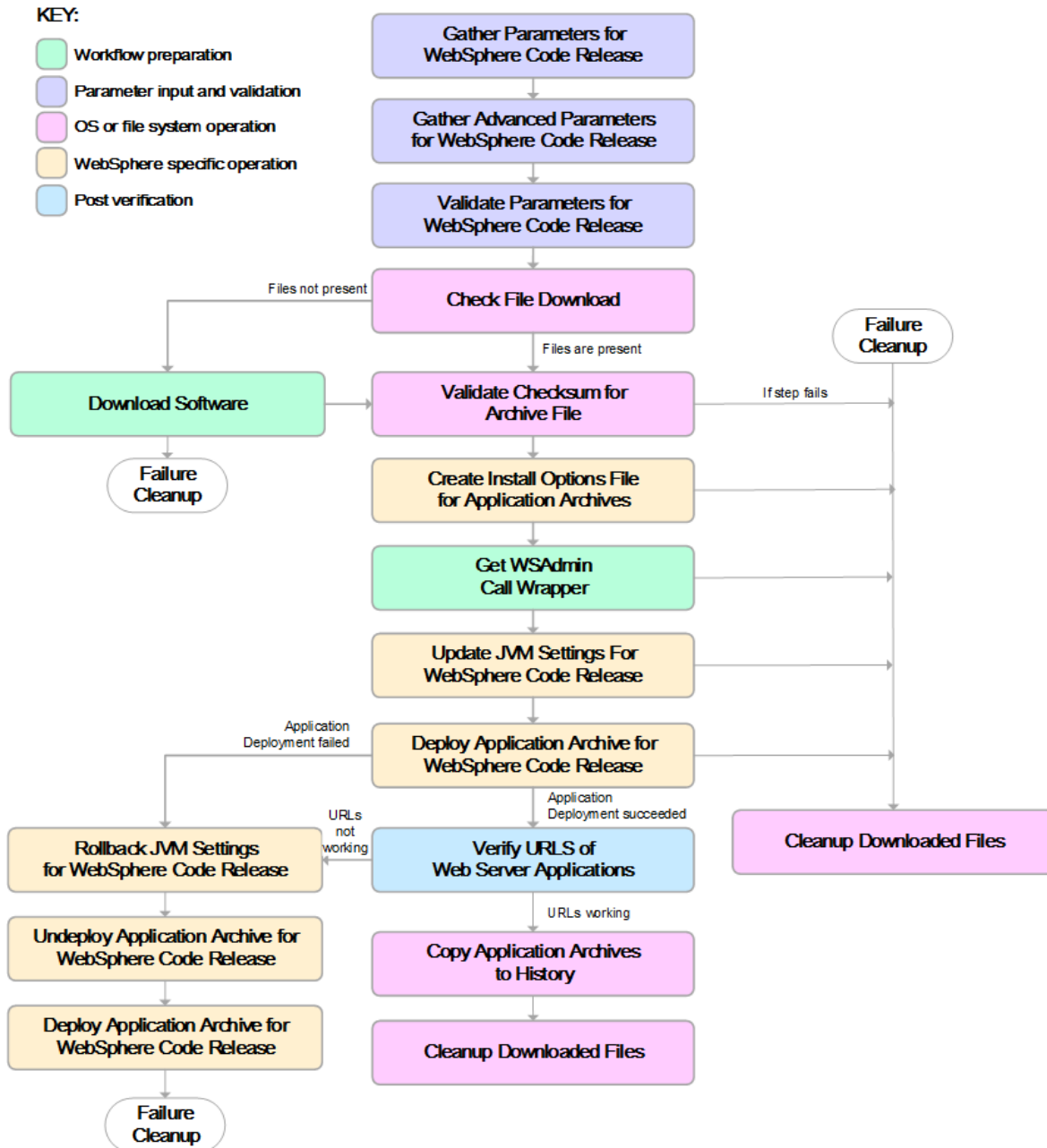
Enable Security	Must be true or false
If Enable Security is true	WebSphere Admin Username must be specified WebSphere Admin Password must be specified
WebSphere Admin Username	Cannot contain the following characters / \ * , : ; = + ? < > & % ' " [] # \$ ^ { } and also cannot begin with a dash (-), period (.), or space ()
WebSphere Admin Password	Cannot begin with a dash (-) and cannot contain a space ()
Code Release Staging Location Code Release History Location	Must be valid absolute paths Cannot have the same values
Application Archive File List Md5 Checksum	There must be a checksum for each Application Archive file The Application Archive files must be type .ear or .war and have valid absolute paths Checksums must be valid hexadecimal numbers

The WebSphere - Code Release workflow also checks the environment for the following:

- The WebSphere container type must be APPLICATION_SERVER.
- The WebSphere Home exists.

Steps Executed

The WebSphere - Code Release workflow includes the following steps. Each step must complete successfully before the next step can start. If a step fails, the workflow reports a failure and subsequent steps are skipped, except for the Cleanup Downloaded Files step.



Steps Used in the WebSphere - Code Release Workflow

Workflow Step	Description
Gather Parameters for WebSphere Code Release	This step gathers mandatory input parameters (user-provided) used to deploy a list of application archives in a IBM WebSphere Application Server on a standalone setup.
Gather Advanced Parameters for WebSphere Code Release	This step gathers the advanced input parameters (user-provided) used to deploy an application archive for a WebSphere Application Server. Input parameters specified in this step are optional. Appropriate default values are specified.
Validate Parameters for WebSphere Code Release	This step validates the basic and advanced parameters provided by the user, and checks the prerequisites for deploying a list of application archives for an IBM WebSphere Application Server on a standalone setup.
Check File Download	<p>This step checks for the existence of a file before downloading from the Server Automation software repository.</p> <ul style="list-style-type: none"> • Checks if file is in the expected location. • If the file is not in the expected location, generates a list of files for file download.
Download Software	This step downloads a list of files to a specified location on the target server.
Validate Checksum for Archive File	This step verifies the checksum for the archive files and archive setting file (if any) to ensure that the file has not changed and that the correct archives are deployed in the Application Server.
Create Install Options File for Application Archives	This step creates a setting file that includes the install options for the list of application archive files being deployed by the application server.
Get WSAdmin Call Wrapper	This step creates the necessary call wrapper to call <code>wsadmin</code> to execute certain operations within a given WebSphere environment.
Update JVM Settings For WebSphere Code Release	This step updates the JVM setting of the IBM WebSphere Application server. It also performs a backup of the IBM WebSphere profile configuration.
Deploy Application Archive for WebSphere Code Release	Using the user-provided Application Archive files: This step deploys the list of application archives in the IBM WebSphere Application Server on a standalone setup.
If the application deployment succeeds, the following steps are executed	
Verify URLs of Web Server Applications	This step verifies that the URLs are working, and looks for return status code values of 200 for success.
Copy Application Archives to History	This step copies the list of files from the staging location to the history location.
Cleanup	For workflow success—and if Cleanup on Success is set to True (default)—

Steps Used in the WebSphere - Code Release Workflow, continued

Workflow Step	Description
Downloaded Files	this step removes all downloaded files and archives. Dependencies: Run as file/directory owner.
If the application deployment fails, the following steps are executed	
Rollback JVM Settings for WebSphere Code Release	This step restores a backup of the IBM WebSphere profile configuration.
Undeploy Application Archive for WebSphere Code Release	This step uninstalls the list of application archives from an IBM WebSphere Application Server on a standalone setup.
Deploy Application Archive for WebSphere Code Release	Using the backup of the Application Archive files: This step deploys the list of application archives in the IBM WebSphere Application Server on a standalone setup.
Cleanup Downloaded Files	For workflow failure—and if Cleanup on Failure is set to True (default)—this step removes all downloaded files and archives. Dependencies: Run as file/directory owner.

For parameter descriptions and defaults, see ["Parameters for WebSphere - Code Release" on page 1355](#).

How to Run this Workflow

The following instructions show you how to customize and run the WebSphere - Code Release workflow in your environment.

The workflow provides default values for some parameters. These default values are usually sufficient for a "typical" installation. You can override the defaults by specifying parameter values in the deployment. For details about specific parameter values, see ["Parameters for WebSphere - Code Release" on page 1355](#).

Note: Before following this procedure, review the ["Prerequisites for this Workflow"](#), and ensure that all requirements are satisfied.

Before you run this workflow, you can perform the following optional advance configuration to deploy applications WebSphere application servers.

Create a configuration file on the target machine or the SA Server. The file should contain the advanced parameters for all the application servers being deployed. If no configuration file is provided, the target will be defaulted to admin server of the domain. The options that are to be used in this file are listed in the table below.


```

AdderEAR.ear = {
  Deploy enterprise beans = No
  Application name = adder_app
}
myServletWAR.war = {
  Deploy enterprise beans = No
  Validate Install = warn
  Precompile JavaServer Pages files = Yes
  Application name = myServletWAR_war
}

```

The options in this file should be in the following format:

Option	Description
Precompile JavaServer Pages files	Specify whether to precompile JavaServer Pages (JSP) files as part of installation. The default is not to precompile JSP files.
Distribute application	The default is to enable application distribution. You can override this and choose to not distribute the application across multiple nodes.
Use Binary Configuration	Specifies whether the application server uses the binding, extensions, and deployment descriptors located with the application deployment document, the deployment.xml file (default), or those located in the EAR file.
Deploy enterprise beans	The tool generates the code needed to

Option	Description
	run enterprise bean (EJB) files. You must enable this setting when the EAR file is assembled and EJBDeploy is not run during packaging. Its default value is false.
Application name	A logical name for the application. The default name is the same as the EAR file. An application name must be unique within the cell.
Create MBeans for resources	Specifies whether to create MBeans for resources, such as servlets or JSP files, within an application when the application starts. The default value is to create MBeans.
Override class reloading settings for Web and EJB modules	Specifies whether the WebSphere Application Server runtime detects changes to application classes when the application is running. If this setting is enabled and if application classes are changed, then the application is stopped and restarted to reload updated classes. The default value is not to enable class reloading.
Reload interval in seconds	Specifies the number of seconds to scan the application's

Option	Description
	file system for updated files.
Process embedded configuration	Specifies whether the embedded configuration should be processed. An embedded configuration consists of files such as <code>resource.xml</code> and <code>variables.xml</code> . When selected or true, the embedded configuration is loaded to the application scope from the <code>.ear</code> file.
File Permission	<ul style="list-style-type: none"> • Allows all files to be read but not written to • Allows executables to execute • Allows HTML and image files to be read by everyone
Application Build ID	A string that identifies the build version of the application. Once it is set, it cannot be modified.
Allow dispatching includes to remote resources	Web modules included in this application are enabled as remote request dispatcher clients that can dispatch remote includes. The default value is true.
Allow servicing includes from remote resources	Web modules included in this application are enabled as remote

Option	Description
	request dispatcher servers that are resolved to service remote includes from another application. The default value is true.
Business level application name	Specifies whether the product creates a new business-level application with the enterprise application that you are installing or makes the enterprise application a composition unit of an existing business-level application.
Asynchronous Request Dispatch Type	Specifies whether the web modules can dispatch requests concurrently on separate threads.
Validate Install	Specifies whether the product examines the application references specified during application installation or updating and, if validation is enabled, warns you of incorrect references or fails the operation.

The value must be separated by an '=' sign, for example: Application name = myServletWAR_war

To use the WebSphere - Code Release workflow:

1. Create a deployable copy of the workflow.
2. Determine the values that you will specify for the following parameters:

Parameters Defined in this Step: Gather Parameters for WebSphere - Code Release

Parameter Name	Default Value	Required	Description
Application Archive File List	no default	required	Comma-separated list of the Application Archive files to be deployed. Example: xxx.war or yyy.ear
Code Release History Location	no default	required	Fully qualified path name of the location where the application archive will be saved (for history purposes) on the target machine. This location cannot be the same as the Code Release Staging Location.
Code Release Staging Location	no default	required	Fully qualified path name of the location where the application archive will be saved on the target machine. This location cannot be the same as the Code Release History Location.
Enable Security	no default	required	Indicates whether security will be enabled. Valid values are True or False. If True then WebSphere Admin Password and WebSphere Admin User must have values.
MD5 Checksum	no default	required	Comma-separated list of the MD5 Checksum of the Application Archive files to be deployed.
Test URLs	no default	required	Comma-separated list of URLs used to test whether or not the list of applications deployed successfully. Example: http://mytestdb.com , http://yourtest.com

Tip: To avoid having to re-enter passwords whenever they change, you can create a policy to provide them to the workflow.

Note: This is the minimum set of parameters required to run this workflow. You may need to expose additional parameters depending on your objectives.

See "[Parameters for WebSphere - Code Release](#)" on [page 1355](#) for detailed descriptions of all input parameters for this workflow, including default values.

3. In the workflow editor, expose any additional parameters that you need. You will specify values for those parameters when you create the deployment
4. Save the changes to the workflow (click **Save** in the lower right corner).
5. Create a new deployment.

6. On the Parameters tab, specify values for the required parameters listed in step 2 and any additional parameters that you have exposed. You do not need to specify values for those parameters whose default values are appropriate for your environment.
7. On the Targets tab, specify one or more targets for this deployment.
8. Save the deployment (click **Save** in the lower right corner).
9. Run the workflow using this deployment.

To verify the results:

The workflow will complete and report SUCCESS on the Console if it has run successfully. If an error occurs during workflow execution, the error is logged, and the workflow terminates in the FAILURE state.

Optional: If you want to further verify the results:

Use the WebSphere administrative console interface to check that the web server is configured.

Sample Scenario

This topic shows you typical parameter values for different use cases for the WebSphere - Code Release workflow. For a complete list of all parameters used in this workflow, including default values, see ["Parameters for WebSphere - Code Release" on page 1355](#).

Tip: To avoid having to re-enter passwords whenever they change, you can create a policy to provide them to the workflow.

Scenario 1: Install an application archive (for example stockanalysis.war) on a running IBM WebSphere Application Server on a standalone setup.

In this scenario we will deploy the stockanalysis.war file on a running IBM WebSphere Application Server. We will install the application using the default installation options. If the application archive files are not present in the Code Release Staging Location, then they will be downloaded from the SA Repository.

Parameters Defined in this Step: Gather Parameters for WebSphere - Code Release

Parameter Name	Example Value	Description
Application Archive File List	stockanalysis.war	Comma-separated list of the Application Archive files to be deployed.

Parameters Defined in this Step: Gather Parameters for WebSphere - Code Release , continued

Parameter Name	Example Value	Description
		Example: xxx.war or yyy.ear
Code Release History Location	/opt/IBM/was/history	Fully qualified path name of the location where the application archive will be saved (for history purposes) on the target machine. This location cannot be the same as the Code Release Staging Location.
Code Release Staging Location	/tmp/IBM/was/staging	Fully qualified path name of the location where the application archive will be saved on the target machine. This location cannot be the same as the Code Release History Location.
Enable Security	False	Indicates whether security will be enabled. Valid values are True or False. If True then WebSphere Admin Password and WebSphere Admin User must have values.
MD5 Checksum	4477e994e9d457ad2214a3d36b1bb16b	Comma-separated list of the MD5 Checksum of the Application Archive files to be deployed.
Test URLs	http://<server:port>/stockanalysis/<xyx.html>	Comma-separated list of URLs used to test whether or not the list of applications deployed successfully. Example: http://mytestdb.com , http://yourtest.com

Scenario 2: Install an application archive (for example stockanalysis.war) on a running IBM WebSphere Application Server on a standalone setup.

In this scenario we will deploy the stockanalysis.war file on a running IBM WebSphere Application Server. We will install the application using the default installation options. The JVM settings are also applied to the Application server. If the application archive files are not present in the Code Release Staging Location, then they will be downloaded from the SA Repository.

Parameters Defined in this Step: Gather Parameters for WebSphere - Code Release

Parameter Name	Example Value	Description
Application Archive File List	stockanalysis.war	Comma-separated list of the Application Archive files to be deployed. Example: xxx.war or yyy.ear

Parameters Defined in this Step: Gather Parameters for WebSphere - Code Release , continued

Parameter Name	Example Value	Description
Code Release History Location	/opt/IBM/was/history	Fully qualified path name of the location where the application archive will be saved (for history purposes) on the target machine. This location cannot be the same as the Code Release Staging Location.
Code Release Staging Location	/tmp/IBM/was/staging	Fully qualified path name of the location where the application archive will be saved on the target machine. This location cannot be the same as the Code Release History Location.
Enable Security	False	Indicates whether security will be enabled. Valid values are True or False. If True then WebSphere Admin Password and WebSphere Admin User must have values.
MD5 Checksum	4477e994e9d457ad2214a3d36b1bb16b	Comma-separated list of the MD5 Checksum of the Application Archive files to be deployed.
Test URLs	http://<server:port>/stockanalysis/<xyx.html>	Comma-separated list of URLs used to test whether or not the list of applications deployed successfully. Example: http://mytestdb.com , http://yourtest.com

Parameters Defined in this Step: Gather Advanced Parameters for WebSphere - Code Release

Parameter Name	Example Value	Description
JVM Generic Arguments	<ul style="list-style-type: none"> Dclient.encoding.override=UTF-8 Dsun.rmi.dgc.client.gcInterval=3600000000 Dsun.rmi.dgc.server.gcInterval=3600000000 	Specifies the JVM generic arguments. Provide values as standard JVM settings.
JVM System Properties	stockanalysis_home, /opt/stockanalysis/bin, Home path for the stock analysis	Specifies the JVM System Properties. Provide the string in the following format: 'PropertyName, PropertyValue PropertyName, PropertyValue'

Scenario 3: Install an application archive (for example stockanalysis.war) on a running IBM WebSphere Application Server on a standalone setup.

In this scenario we deploy the stockanalysis.war file on a running IBM WebSphere Application Server. We will install the application using the default installation options. This scenario provides the install options to deploy the application archive in a file. If the Application Archive Files and the Archive Setting File are not present in the Code Release Staging Location, then they will be downloaded from the SA Repository.

Parameters Defined in this Step: Gather Parameters for WebSphere - Code Release

Parameter Name	Example Value	Description
Application Archive File List	stockanalysis.war	Comma-separated list of the Application Archive files to be deployed. Example: xxx.war or yyy.ear
Code Release History Location	/opt/IBM/was/history	Fully qualified path name of the location where the application archive will be saved (for history purposes) on the target machine. This location cannot be the same as the Code Release Staging Location.
Code Release Staging Location	/tmp/IBM/was/staging	Fully qualified path name of the location where the application archive will be saved on the target machine. This location cannot be the same as the Code Release History Location.
Enable Security	False	Indicates whether security will be enabled. Valid values are True or False. If True then WebSphere Admin Password and WebSphere Admin User must have values.
MD5 Checksum	4477e994e9d457ad2214a3d36b1bb16, 1eff908bedaa416c104f6b4a9a268233	Comma-separated list of the MD5 Checksum of the Application Archive files to be deployed.
Test URLs	http://<server:port>/stock/<xyx.html>	Comma-separated list of URLs used to test whether or not the list of applications deployed successfully. Example: http://mytestdb.com , http://yourtest.com

Parameters Defined in this Step: Gather Advanced Parameters for WebSphere - Code Release

Parameter Name	Example Value	Description
Archive Settings File	archive.setting	The file containing the install options for all the archive files. Sample Archive Settings File content:

Parameters Defined in this Step: Gather Advanced Parameters for WebSphere - Code Release, continued

Parameter Name	Example Value	Description
		<pre>stockanalysis.war = { Precompile JavaServer Pages files = No -contextroot /stock }</pre> <p>Options for providing the key are:</p> <ul style="list-style-type: none"> Provide the key in plain English. The key supported is the parameter name in the step Gather Advanced Parameters for WebSphere Code Release. The parameter should be provided without the Archive Install Option (for example, the parameter Archive Install Option Precompile JavaServer Pages is provided in the file as Precompile JavaServer Pages files). Provide the key and value as supported by IBM WebSphere. For example, -contextroot /stock

Parameters for WebSphere - Code Release

The following tables describe the required and optional input parameters for this workflow. For most parameters, if you do not specify a value for a parameter, a default value is assigned.

Parameters Defined in this Step: Gather Parameters for WebSphere - Code Release

Parameter Name	Default Value	Required	Description
Application Archive File List	no default	required	Comma-separated list of the Application Archive files to be deployed. Example: xxx.war or yyy.ear
Code Release History Location	no default	required	Fully qualified path name of the location where the application archive will be saved (for history purposes) on the target machine. This location cannot be the same as the Code Release Staging Location.
Code Release Staging Location	no default	required	Fully qualified path name of the location where the application archive will be saved on the target machine. This location cannot be the same as the Code Release History Location.
Enable Security	no default	required	Indicates whether security will be enabled. Valid values are True or False. If True then WebSphere Admin Password and WebSphere Admin User must have values.

Parameters Defined in this Step: Gather Parameters for WebSphere - Code Release , continued

Parameter Name	Default Value	Required	Description
MD5 Checksum	no default	required	Comma-separated list of the MD5 Checksum of the Application Archive files to be deployed.
Test URLs	no default	required	Comma-separated list of URLs used to test whether or not the list of applications deployed successfully. Example: http://mytestdb.com , http://yourtest.com

Parameters Defined in this Step: Gather Advanced Parameters for WebSphere - Code Release

Parameter Name	Default Value	Required	Description
Archive Install Option Allow Dispatching Includes to Remote Resources	no default	optional	Specifies whether or not an application can dispatch includes to resources across web modules in different Java virtual machines in a managed node environment through the standard request dispatcher mechanism. Possible values are Yes or No.
Archive Install Option Allow Servicing Includes from Remote Resources	no default	optional	Specifies whether or not an enterprise application can service an include request from an application. Possible values are Yes or No.
Archive Install Option Application Build ID	no default	optional	Specifies an uneditable string that identifies the Build ID version of the application.
Archive Install Option Asynchronous Request Dispatch Type	no default	optional	Specifies whether or not web modules can dispatch requests concurrently on separate threads, and if so, whether the server or client dispatches the requests. Concurrent dispatching can improve servlet response time.
Archive Install Option Business Level Application Name	no default	optional	Specifies that either the product creates a new business-level application name with the enterprise application that you are installing, or, makes the enterprise application a composition unit of an existing business-level application.
Archive Install Option Create MBeans for Resources	no default	optional	Specifies whether or not to create MBeans for resources such as servlets or JSP files within an application when the application starts. The default behavior is to create MBeans. Possible values are Yes or No.
Archive Install Option Deploy Enterprise Beans	no default	optional	Specifies whether or not the EJBDploy tool runs during application installation. Possible values are Yes or No.

Parameters Defined in this Step: Gather Advanced Parameters for WebSphere - Code Release , continued

Parameter Name	Default Value	Required	Description
Archive Install Option Distribute Application	no default	optional	Specifies whether or not the product expands application binaries in the installation location during installation and deletes application binaries during uninstallation. The default is to enable application distribution. Application binaries for installed applications are expanded to the directory specified. Possible values are Yes or No.
Archive Install Option File Permission	no default	optional	Specifies access permissions for application binaries for installed applications that are expanded to the directory specified. Possible values are .*=755 or .*\..dll=755#.*\..so=755#.*\..a=755#.*\..sl=755 or .*\..htm=755#.*\..html=755#.*\..gif=755#.*\..jpg=755
Archive Install Option Override Class Reloading Settings for Web and EJB Modules	no default	optional	Specifies whether or not the product run time detects changes to application classes when the application is running. If enabled, and application classes are changed, then the application is stopped and restarted to reload updated classes. Possible values are Yes or No.
Archive Install Option Precompile JavaServer Pages Files	no default	optional	Specifies whether or not to precompile JavaServer Pages (JSP) files as a part of installation. The default is not to precompile JSP files. Possible values are Yes or No.
Archive Install Option Process Embedded Configuration	no default	optional	Specifies whether or not the embedded configuration should be processed. An embedded configuration consists of files such as resource.xml, variables.xml, and deployment.xml. You can collect WebSphere Application Server-specific deployment information and store it in the application EAR file. You can then install the EAR file into a WebSphere Application Server configuration using application management interfaces. Possible values are Yes or No.
Archive Install Option Reload Interval in Seconds	no default	optional	Specifies the number of seconds to scan the application's file system for updated files. The default is the value of the reloading interval attribute in the IBM extension (META-INF/ibm-application-ext.xml) file of the EAR file. The reloading interval attribute takes effect only if class reloading is enabled. To enable reloading, specify a value greater than zero (for example, 1 to 2147483647). To disable reloading, specify zero (0). The range is from 0 to 2147483647.
Archive Install Option Use Binary Configuration	no default	optional	Specifies whether or not the application server uses the binding, extensions, and deployment descriptors located with the application

Parameters Defined in this Step: Gather Advanced Parameters for WebSphere - Code Release, continued

Parameter Name	Default Value	Required	Description
			deployment document, the deployment.xml file (default), or those located in the enterprise archive (EAR) file. Select this setting for applications installed on Version 6.0 or later deployment targets only. Possible values are Yes or No.
Archive Install Option Validate Install	no default	optional	Specifies whether or not the product examines the application references specified during application installation or updating and, if validation is enabled, warns users about incorrect references or fails the operation. Valid values are Off, Warn and Fail. Specify Off for no resource validation, Warn for warning messages about incorrect resource references, or Fail to stop operations that fail as a result of incorrect resource references.
Archive Settings File	no default	optional	The file containing the install options for all the archive files.
Cleanup on Failure	True	optional	Determines whether or not to remove downloaded and extracted files. This parameter also cleans up the installed directory upon failure of the workflow.
Cleanup on Success	True	optional	Determines whether or not to remove downloaded and extracted files. This parameter also cleans up the installed directory upon successful execution of the workflow.
JVM Generic Arguments	no default	optional	Specifies the JVM generic arguments. Provide values as standard JVM settings.
JVM System Properties	no default	optional	Specifies the JVM System Properties. Provide the string in the following format: 'PropertyName, PropertyValue PropertyName, PropertyValue'
Web Service Password	no default	required	Password for the Web Service API.
Web Service URL	dma.url	required	URL for the DMA Discovery web service API. Example: https://example.com/8443/dma
Web Service User	dma.user	required	A user capable of modifying the DMA managed environment by using the web service API.
WebSphere Admin Password	no default	optional	The password for a user in a group that can change the state of a given application server. Only required if global security is enabled. It cannot not begin with a dash (-) or contain a space ().
WebSphere Admin	no default	optional	The user account for a user in a group that can

Parameters Defined in this Step: Gather Advanced Parameters for WebSphere - Code Release, continued

Parameter Name	Default Value	Required	Description
Username			change the state of a given application server. Only required if global security is enabled. It cannot begin with a dash (-), a period (.), or a space (.). It cannot contain any of the following characters / \ * , : ; = + ? < > & % ' " [] # \$ ^ { }.

WebSphere - Code Release on Cluster

This workflow automates the deployment of applications in IBM WebSphere. In addition to deployment, this workflow can update the JVM Generic Arguments and JVM System Properties on the Web Server, and also provides install options for the deployment of applications.

Some of the install options are provided as parameters to the workflow, or users can specify install options within a file for each of the applications to be deployed. Note, though, that the value provided for parameters takes higher precedence. This workflow supports the verification of the application deployments by providing the URLs.

For successful application deployments, verifications and a list of the applications are maintained in the History file. In cases of unsuccessful application deployments, the workflow rolls back the deployment and restores the last successfully deployed application (if any).

To use this workflow in your environment, see the following information:

Topic	Information Included
"Prerequisites for this Workflow"	List of prerequisites that must be satisfied before you can run this workflow
"How this Workflow Works"	Information about what the workflow does, including validation checks performed, steps executed, and a high-level process flow
"How to Run this Workflow"	Instructions for running this workflow in your environment
"Sample Scenario"	Examples of typical parameter values for this workflow
Parameters	List of input parameters for this workflow

Prerequisites for this Workflow

Be sure that the following prerequisites are satisfied before you run the WebSphere - Code Release on Cluster workflow.

Product Platform

This workflow automates application deployments in IBM WebSphere 8 or WebSphere 8.5.x.

Dependencies

This workflow has the following dependencies:

- A working WebSphere Network Deployment cell, whose Deployment Manager is available for communication
- You must run the Discover WebSphere workflow before running this workflow. The Discover WebSphere workflow audits the server's physical environment for WebSphere cells, clusters, and application servers and then stores the configuration information in the DMA environment.

For more information about prerequisites for WebSphere, refer to the [WebSphere 8 Product Documentation](#).

How this Workflow Works

The following information describes how the WebSphere - Code Release On Cluster workflow works:

Overview

This workflow does the following things in the order shown:

1. Initially, the workflow inputs all parameters, set defaults for optional parameters, validates all parameters, and determines all members of the cluster. If input files do not exist in the specified locations, they are downloaded from the software repository. The workflow performs a checksum to verify that the archive files should be deployed in the Application Server on a cluster setup.
2. Next, the workflow creates the installation options and the call wrapper that will be used to execute commands within a WebSphere environment. The workflow updates the JVM setting and then creates a backup. The workflow deploys the specified Application Archive files in the Application Server on a cluster setup.
3. If the application deployment succeeds, the workflow tests the URLs for the web servers and copies the application archives.
4. If the application deployment fails, the workflow rolls back the deployment and restores the last successfully deployed application (if any).
5. Finally, the workflow cleans up downloaded files based on the Cleanup on Success and Cleanup on Failure parameters.

Validation Checks Performed

The workflow performs the following checks on the input parameters:

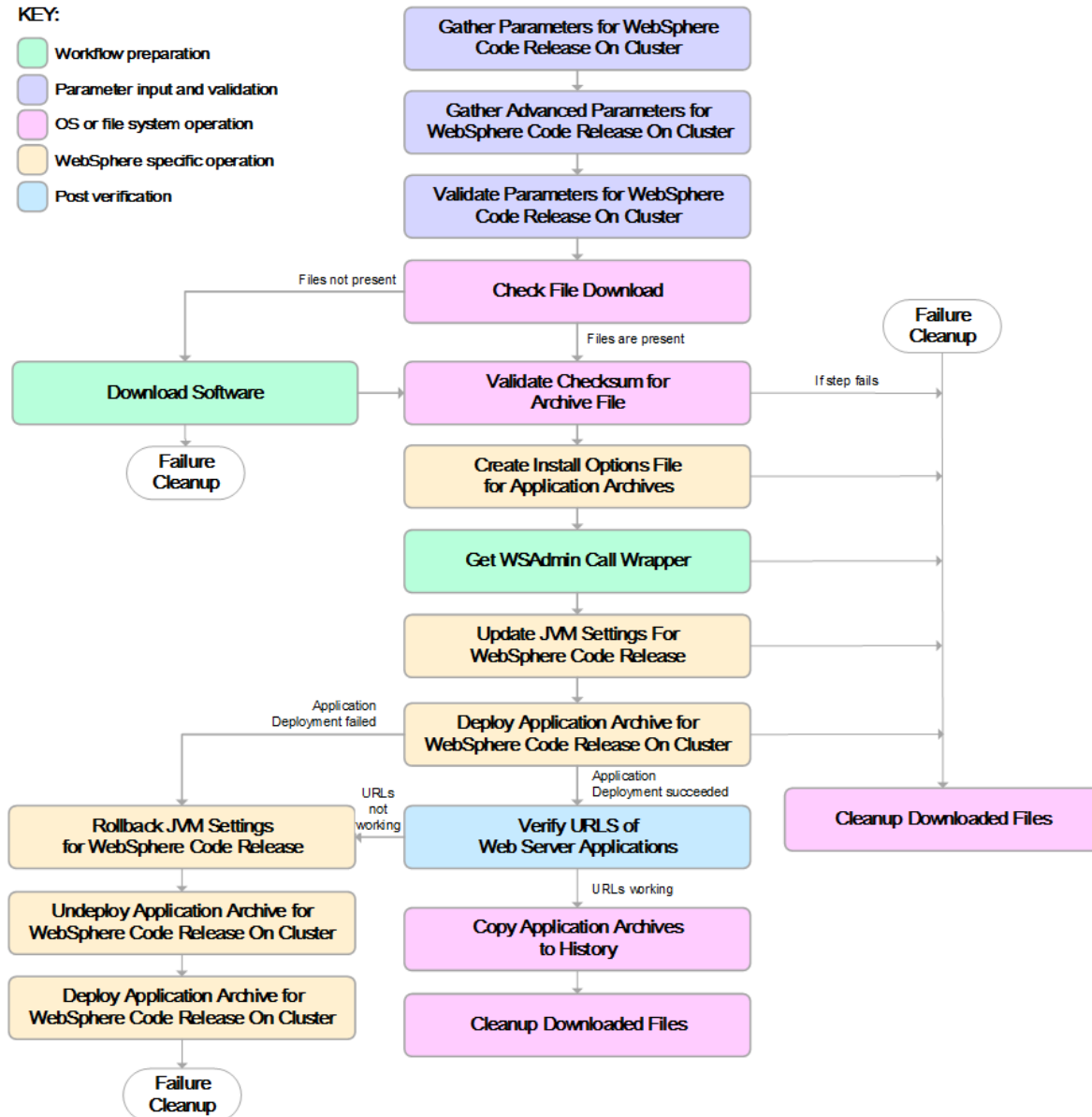
Enable Security	Must be true or false
If Enable Security is true	WebSphere Admin Username must be specified WebSphere Admin Password must be specified
WebSphere Admin Username	Cannot contain the following characters / \ * , : ; = + ? < > & % ' " [] # \$ ^ { } and also cannot begin with a dash (-), period (.), or space ()
WebSphere Admin Password	Cannot begin with a dash (-) and cannot contain a space ()
Code Release Staging Location Code Release History Location	Must be valid absolute paths Cannot have the same values
Application Archive File List Md5 Checksum	There must be a checksum for each Application Archive file The Application Archive files must be type .ear or .war and have valid absolute paths Checksums must be valid hexadecimal numbers

The WebSphere - Code Release On Cluster workflow also checks the environment for the following:

- The WebSphere container type must be cluster.
- The WebSphere Home exists.

Steps Executed

The workflow includes the following steps. Each step must complete successfully before the next step can start. If a step fails, the workflow reports a failure and subsequent steps are skipped, except for the Cleanup Downloaded Files step.



Steps Used in the WebSphere - Code Release Workflow

Workflow Step	Description
Gather Parameters for WebSphere Code Release On Cluster	This step gathers mandatory input parameters (user-provided) used to deploy a list of application archives in a IBM WebSphere Application Server on a cluster setup.
Gather Advanced Parameters for WebSphere Code Release On Cluster	This step gathers the advanced input parameters (user-provided) used to deploy an application archive for a WebSphere Application Server on a cluster setup. Input parameters specified in this step are optional. Appropriate default values are specified.
Validate Parameters for WebSphere Code Release On Cluster	This step validates the basic and advanced parameters provided by the user, and checks the prerequisites for deploying a list of application archives for an IBM WebSphere Application Server on a cluster setup.
Check File Download	<p>This step checks for the existence of a file before downloading from the Server Automation software repository.</p> <ul style="list-style-type: none"> • Checks if file is in the expected location. • If the file is not in the expected location, generates a list of files for file download.
Download Software	This step downloads a list of files to a specified location on the target server.
Validate Checksum for Archive File	This step verifies the checksum for the archive files and archive setting file (if any) to ensure that the file has not changed and that the correct archives are deployed in the Application Server.
Create Install Options File for Application Archives	This step creates a setting file that includes the install options for the list of application archive files being deployed by the application server.
Get WSAAdmin Call Wrapper	This step creates the necessary call wrapper to call <code>wsadmin</code> to execute certain operations within a given WebSphere environment.
Update JVM Settings For WebSphere Code Release	This step updates the JVM setting of the IBM WebSphere Application server. It also performs a backup of the IBM WebSphere profile configuration.
Deploy Application Archive for WebSphere Code Release On Cluster	Using the user-provided Application Archive files: This step deploys the list of application archives in the IBM WebSphere Application Server on a cluster setup.

Steps Used in the WebSphere - Code Release Workflow, continued

Workflow Step	Description
If the application deployment succeeds, the following steps are executed	
Verify URLs of Web Server Applications	This step verifies that the URLs are working, and looks for return status code values of 200 for success.
Copy Application Archives to History	This step copies the list of files from the staging location to the history location.
Cleanup Downloaded Files	For workflow success—and if Cleanup on Success is set to True (default)—this step removes all downloaded files and archives. Dependencies: Run as file/directory owner.
If the application deployment fails, the following steps are executed	
Rollback JVM Settings for WebSphere Code Release	This step restores a backup of the IBM WebSphere profile configuration.
Undeploy Application Archive for WebSphere Code Release On Cluster	This step uninstalls the list of application archives from a IBM WebSphere Application Server on a cluster setup.
Deploy Application Archive for WebSphere Code Release	Using the backup of the Application Archive files: This step deploys the list of application archives in the IBM WebSphere Application Server on a cluster setup.
Cleanup Downloaded Files	For workflow failure—and if Cleanup on Failure is set to True (default)—this step removes all downloaded files and archives. Dependencies: Run as file/directory owner.

For parameter descriptions and defaults, see ["Parameters for WebSphere - Code Release on Cluster" on page 1370](#).

How to Run this Workflow

The following instructions show you how to customize and run the WebSphere - Code Release on Cluster workflow in your environment.

The workflow provides default values for some parameters. These default values are usually sufficient for a "typical" installation. You can override the defaults by specifying parameter values in the deployment.

Note: Before following this procedure, review the [Prerequisites for this Workflow](#), and ensure that all requirements are satisfied.

To use the WebSphere - Code Release on Cluster workflow:

1. Create a deployable copy of the workflow.
2. Determine the values that you will specify for the following parameters:

Parameters Defined in this Step: Gather Parameters for WebSphere - Code Release

Parameter Name	Default Value	Required	Description
Application Archive File List	no default	required	Comma-separated list of the Application Archive files to be deployed. Example: xxx.war or yyy.ear
Code Release History Location	no default	required	Fully qualified path name of the location where the application archive will be saved (for history purposes) on the target machine. This location cannot be the same as the Code Release Staging Location.
Code Release Staging Location	no default	required	Fully qualified path name of the location where the application archive will be saved on the target machine. This location cannot be the same as the Code Release History Location.
Enable Security	no default	required	Indicates whether security will be enabled. Valid values are True or False. If True then WebSphere Admin Password and WebSphere Admin User must have values.
MD5 Checksum	no default	required	Comma-separated list of the MD5 Checksum of the Application Archive files to be deployed.
Test URLs	no default	required	Comma-separated list of URLs used to test whether or not the list of applications deployed successfully. Example: http://mytestdb.com , http://yourtest.com

Tip: To avoid having to re-enter passwords whenever they change, you can create a policy to provide them to the workflow.

Note: This is the minimum set of parameters required to run this workflow. You may need to expose additional parameters depending on your objectives.

See ["Parameters for WebSphere - Code Release on Cluster" on page 1370](#) for detailed descriptions of all input parameters for this workflow, including default values.

3. In the workflow editor, expose any additional parameters that you need. You will specify values for those parameters when you create the deployment
4. Save the changes to the workflow (click **Save** in the lower right corner).

5. Create a new deployment.
6. On the Parameters tab, specify values for the required parameters listed in step 2 and any additional parameters that you have exposed. You do not need to specify values for those parameters whose default values are appropriate for your environment.
7. On the Targets tab, specify one or more targets for this deployment.
8. Save the deployment (click **Save** in the lower right corner).
9. Run the workflow using this deployment.

To verify the results:

The workflow will complete and report SUCCESS on the Console if it has run successfully. If an error occurs during workflow execution, the error is logged, and the workflow terminates in the FAILURE state.

Optional: If you want to further verify the results:

Use the WebSphere administrative console interface to check that the web server is configured.

Sample Scenario

This topic shows you typical parameter values for different use cases for the WebSphere - Code Release on Cluster workflow. For a complete list of all parameters used in this workflow, including default values, see ["Parameters for WebSphere - Code Release on Cluster" on page 1370](#).

Tip: To avoid having to re-enter passwords whenever they change, you can create a policy to provide them to the workflow.

Scenario 1: Install an application archive (for example stockanalysis.war) on a running IBM WebSphere Application Server on a standalone setup.

In this scenario we will deploy the stockanalysis.war file on a running IBM WebSphere Application Server. We will install the application using the default installation options. If the application archive files are not present in the Code Release Staging Location, then they will be downloaded from the SA Repository.

Parameters Defined in this Step: Gather Parameters for WebSphere - Code Release

Parameter Name	Default Value	Description
Application Archive File List	stockanalysis.war	Comma-separated list of the Application Archive files to be deployed.

Parameters Defined in this Step: Gather Parameters for WebSphere - Code Release , continued

Parameter Name	Default Value	Description
		Example: xxx.war or yyy.ear
Code Release History Location	/opt/IBM/was/history	Fully qualified path name of the location where the application archive will be saved (for history purposes) on the target machine. This location cannot be the same as the Code Release Staging Location.
Code Release Staging Location	/tmp/IBM/was/staging	Fully qualified path name of the location where the application archive will be saved on the target machine. This location cannot be the same as the Code Release History Location.
Enable Security	False	Indicates whether security will be enabled. Valid values are True or False. If True then WebSphere Admin Password and WebSphere Admin User must have values.
MD5 Checksum	4477e994e9d457ad2214a3d36b1bb16b	Comma-separated list of the MD5 Checksum of the Application Archive files to be deployed.
Test URLs	http://<server:port>/stockanalysis/<xyx.html>	Comma-separated list of URLs used to test whether or not the list of applications deployed successfully. Example: http://mytestdb.com , http://yourtest.com

Scenario 2: Install an application archive (for example stockanalysis.war) on a running IBM WebSphere Application Server on a standalone setup.

In this scenario we will deploy the stockanalysis.war file on a running IBM WebSphere Application Server. We will install the application using the default installation options. The JVM settings are also applied to the Application server. If the application archive files are not present in the Code Release Staging Location, then they will be downloaded from the SA Repository.

Parameters Defined in this Step: Gather Parameters for WebSphere - Code Release

Parameter Name	Default Value	Description
Application Archive File List	stockanalysis.war	Comma-separated list of the Application Archive files to be deployed. Example: xxx.war or yyy.ear

Parameters Defined in this Step: Gather Parameters for WebSphere - Code Release , continued

Parameter Name	Default Value	Description
Code Release History Location	/opt/IBM/was/history	Fully qualified path name of the location where the application archive will be saved (for history purposes) on the target machine. This location cannot be the same as the Code Release Staging Location.
Code Release Staging Location	/tmp/IBM/was/staging	Fully qualified path name of the location where the application archive will be saved on the target machine. This location cannot be the same as the Code Release History Location.
Enable Security	False	Indicates whether security will be enabled. Valid values are True or False. If True then WebSphere Admin Password and WebSphere Admin User must have values.
MD5 Checksum	4477e994e9d457ad2214a3d36b1bb16b	Comma-separated list of the MD5 Checksum of the Application Archive files to be deployed.
Test URLs	http://<server:port>/stockanalysis/<xyx.html>	Comma-separated list of URLs used to test whether or not the list of applications deployed successfully. Example: http://mytestdb.com , http://yourtest.com

Parameters Defined in this Step: Gather Advanced Parameters for WebSphere - Code Release

Parameter Name	Default Value	Description
JVM Generic Arguments	<ul style="list-style-type: none"> Dclient.encoding.override=UTF-8 Dsun.rmi.dgc.client.gcInterval=3600000000 Dsun.rmi.dgc.server.gcInterval=3600000000 	Specifies the JVM generic arguments. Provide values as standard JVM settings.
JVM System Properties	stockanalysis_home, /opt/stockanalysis/bin, Home path for the stock analysis	Specifies the JVM System Properties. Provide the string in the following format: 'PropertyName, PropertyValue PropertyName, PropertyValue'

Scenario 3: Install an application archive (for example stockanalysis.war) on a running IBM WebSphere Application Server on a standalone setup.

In this scenario we deploy the stockanalysis.war file on a running IBM WebSphere Application Server. We will install the application using the default installation options. This scenario provides the install options to deploy the application archive in a file. If the Application Archive Files and the Archive Setting File are not present in the Code Release Staging Location, then they will be downloaded from the SA Repository.

Parameters Defined in this Step: Gather Parameters for WebSphere - Code Release

Parameter Name	Default Value	Description
Application Archive File List	stockanalysis.war	Comma-separated list of the Application Archive files to be deployed. Example: xxx.war or yyy.ear
Code Release History Location	/opt/IBM/was/history	Fully qualified path name of the location where the application archive will be saved (for history purposes) on the target machine. This location cannot be the same as the Code Release Staging Location.
Code Release Staging Location	/tmp/IBM/was/staging	Fully qualified path name of the location where the application archive will be saved on the target machine. This location cannot be the same as the Code Release History Location.
Enable Security	False	Indicates whether security will be enabled. Valid values are True or False. If True then WebSphere Admin Password and WebSphere Admin User must have values.
MD5 Checksum	4477e994e9d457ad2214a3d36b1bb16, 1eff908bedaa416c104f6b4a9a268233	Comma-separated list of the MD5 Checksum of the Application Archive files to be deployed.
Test URLs	http://<server:port>/stock/<xyx.html>	Comma-separated list of URLs used to test whether or not the list of applications deployed successfully. Example: http://mytestdb.com , http://yourtest.com

Parameters Defined in this Step: Gather Advanced Parameters for WebSphere - Code Release

Parameter Name	Default Value	Description
Archive Settings File	archive.setting	The file containing the install options for all the archive files. Sample Archive Settings File content: stockanalysis.war = { Precompile JavaServer Pages files = No -contextroot /stock

Parameters Defined in this Step: Gather Advanced Parameters for WebSphere - Code Release, continued

Parameter Name	Default Value	Description
		<p>}</p> <p>Options for providing the key are:</p> <ul style="list-style-type: none"> Provide the key in plain English. The key supported is the parameter name in the step Gather Advanced Parameters for WebSphere Code Release. The parameter should be provided without the Archive Install Option (for example, the parameter Archive Install Option Precompile JavaServer Pages is provided in the file as Precompile JavaServer Pages files). Provide the key and value as supported by IBM WebSphere. For example, - contextroot /stock

Parameters for WebSphere - Code Release on Cluster

The following tables describe the required and optional input parameters for this workflow. For most parameters, if you do not specify a value for a parameter, a default value is assigned.

Parameters Defined in this Step: Gather Parameters for WebSphere - Code Release on Cluster

Parameter Name	Default Value	Required	Description
Application Archive File List	no default	required	Comma-separated list of the Application Archive files to be deployed. Example: xxx.war or yyy.ear
Code Release History Location	no default	required	Fully qualified path name of the location where the application archive will be saved (for history purposes) on the target machine. This location cannot be the same as the Code Release Staging Location.
Code Release Staging Location	no default	required	Fully qualified path name of the location where the application archive will be saved on the target machine. This location cannot be the same as the Code Release History Location.
Enable Security	no default	required	Indicates whether security will be enabled. Valid values are True or False. If True then WebSphere Admin Password and WebSphere Admin User must have values.
MD5 Checksum	no default	required	Comma-separated list of the MD5 Checksum of the Application Archive files to be deployed.
Test URLs	no default	required	Comma-separated list of URLs used to test whether or not the list of applications deployed

Parameters Defined in this Step: Gather Parameters for WebSphere - Code Release on Cluster, continued

Parameter Name	Default Value	Required	Description
			successfully. Example: http://mytestdb.com , http://yourtest.com

Parameters Defined in this Step: Gather Advanced Parameters for WebSphere - Code Release on Cluster

Parameter Name	Default Value	Required	Description
Archive Install Option Allow Dispatching Includes to Remote Resources	no default	optional	Specifies whether or not an application can dispatch includes to resources across web modules in different Java virtual machines in a managed node environment through the standard request dispatcher mechanism. Possible values are Yes or No.
Archive Install Option Allow Servicing Includes from Remote Resources	no default	optional	Specifies whether or not an enterprise application can service an include request from an application. Possible values are Yes or No.
Archive Install Option Application Build ID	no default	optional	Specifies an uneditable string that identifies the Build ID version of the application.
Archive Install Option Asynchronous Request Dispatch Type	no default	optional	Specifies whether or not web modules can dispatch requests concurrently on separate threads, and if so, whether the server or client dispatches the requests. Concurrent dispatching can improve servlet response time.
Archive Install Option Business Level Application Name	no default	optional	Specifies that either the product creates a new business-level application name with the enterprise application that you are installing, or, makes the enterprise application a composition unit of an existing business-level application.
Archive Install Option Create MBeans for Resources	no default	optional	Specifies whether or not to create MBeans for resources such as servlets or JSP files within an application when the application starts. The default behavior is to create MBeans. Possible values are Yes or No.
Archive Install Option Deploy Enterprise Beans	no default	optional	Specifies whether or not the EJBDeploy tool runs during application installation. Possible values are Yes or No.
Archive Install Option	no default	optional	Specifies whether or not the product expands application

Parameters Defined in this Step: Gather Advanced Parameters for WebSphere - Code Release on Cluster, continued

Parameter Name	Default Value	Required	Description
Distribute Application			binaries in the installation location during installation and deletes application binaries during uninstallation. The default is to enable application distribution. Application binaries for installed applications are expanded to the directory specified. Possible values are Yes or No.
Archive Install Option File Permission	no default	optional	Specifies access permissions for application binaries for installed applications that are expanded to the directory specified. Possible values are <code>.*=755</code> or <code>.*\.dll=755#.*\so=755#.*\a=755#.*\sl=755</code> or <code>.*\htm=755#.*\html=755#.*\gif=755#.*\jpg=755</code>
Archive Install Option Override Class Reloading Settings for Web and EJB Modules	no default	optional	Specifies whether or not the product run time detects changes to application classes when the application is running. If enabled, and application classes are changed, then the application is stopped and restarted to reload updated classes. Possible values are Yes or No.
Archive Install Option Precompile JavaServer Pages Files	no default	optional	Specifies whether or not to precompile JavaServer Pages (JSP) files as a part of installation. The default is not to precompile JSP files. Possible values are Yes or No.
Archive Install Option Process Embedded Configuration	no default	optional	Specifies whether or not the embedded configuration should be processed. An embedded configuration consists of files such as <code>resource.xml</code> , <code>variables.xml</code> , and <code>deployment.xml</code> . You can collect WebSphere Application Server-specific deployment information and store it in the application EAR file. You can then install the EAR file into a WebSphere Application Server configuration using application management interfaces. Possible values are Yes or No.
Archive Install Option Reload Interval in Seconds	no default	optional	Specifies the number of seconds to scan the application's file system for updated files. The default is the value of the reloading interval attribute in the IBM extension (<code>META-INF/ibm-application-ext.xmi</code>) file of the EAR file. The reloading interval attribute takes effect only if class reloading is enabled. To enable reloading, specify a value greater than zero (for example, 1 to 2147483647). To disable reloading, specify zero (0). The range is from 0 to 2147483647.
Archive Install Option Use Binary Configuration	no default	optional	Specifies whether or not the application server uses the binding, extensions, and deployment descriptors located with the application deployment document, the <code>deployment.xml</code> file (default), or those located in the enterprise archive (EAR) file. Select this setting for applications installed on Version 6.0 or later deployment targets only. Possible values are Yes or No.
Archive Install	no	optional	Specifies whether or not the product examines the

Parameters Defined in this Step: Gather Advanced Parameters for WebSphere - Code Release on Cluster, continued

Parameter Name	Default Value	Required	Description
Option Validate Install	default		application references specified during application installation or updating and, if validation is enabled, warns users about incorrect references or fails the operation. Valid values are Off, Warn and Fail. Specify Off for no resource validation, Warn for warning messages about incorrect resource references, or Fail to stop operations that fail as a result of incorrect resource references.
Archive Settings File	no default	optional	The file containing the install options for all the archive files.
Cleanup on Failure	True	optional	Determines whether or not to remove downloaded and extracted files. This parameter also cleans up the installed directory upon failure of the workflow.
Cleanup on Success	True	optional	Determines whether or not to remove downloaded and extracted files. This parameter also cleans up the installed directory upon successful execution of the workflow.
JVM Generic Arguments	no default	optional	Specifies the JVM generic arguments. Provide values as standard JVM settings.
JVM System Properties	no default	optional	Specifies the JVM System Properties. Provide the string in the following format: 'PropertyName, PropertyValue PropertyName, PropertyValue'
Web Service Password	no default	required	Password for the Web Service API.
Web Service URL	dma.url	required	URL for the DMA Discovery web service API. Example: https://example.com/8443/dma
Web Service User	dma.user	required	A user capable of modifying the DMA managed environment by using the web service API.
WebSphere Admin Password	no default	optional	The password for a user in a group that can change the state of a given application server. Only required if global security is enabled. It cannot not begin with a dash (-) or contain a space ().
WebSphere Admin Username	no default	optional	The user account for a user in a group that can change the state of a given application server. Only required if global security is enabled. It cannot begin with a dash (-), a period (.), or a space (). It cannot contain any of the following characters / \ * , ; : = + ? < > & % ' " [] # \$ ^ { }.

WebSphere 8 - Patch Network Cell

The workflow supports the patching of WebSphere 8.0 or 8.5.x running in a Network Deployment topology and standalone profile. This workflow patches WebSphere 8 instances which are installed by root as well as non-root users. For non-root user installation, patching step of the workflow will run as the user account that has installed WebSphere 8.

Fixes and updates are installed by the workflow using an existing instance of the IBM Installation Manager software, which must exist on each target machine.

This workflow takes into account the multiple components related to a Network Deployment implementation and makes sure that all components (dmgr, nodeagent, and application servers) are stopped before proceeding with the patching.

To use this workflow in your environment, see the following information:

Topic	Information Included
"Prerequisites for this Workflow"	List of prerequisites that must be satisfied before you can run this workflow
"How this Workflow Works"	Information about what the workflow does, including validation checks performed, steps executed, and a high-level process flow
"How to Run this Workflow "	Instructions for running this workflow in your environment
"Sample Scenario"	Examples of typical parameter values for this workflow
Parameters	List of input parameters for this workflow

Prerequisites for this Workflow

Be sure that the following prerequisites are satisfied before you run this workflow:

1. You have installed the DMA Database Release Management solution pack.
2. You have a valid HP Software support contract for this solution pack.
3. You have downloaded and installed all available DMA patches and hot fixes.
4. IBM Installation Manager software exists on each target machine.

For specific target operating system versions supported by each workflow, see the *Database and Middleware Automation Support Matrix* available on the Software Support web site:

<https://softwaresupport.hp.com/>

Dependencies:

- This workflow runs as root. However, it will patch a non-root WebSphere 8.0 or 8.5.x Installation. The workflow runs the patch step as the user that installed WebSphere 8.0 or 8.5.x (installed user).
- The workflow supports the patching of WebSphere 8.0 or 8.5.x running in a Network Deployment topology and standalone profile.
- When patching a Network Deployment Cell, the workflow must be set up to first patch the server that runs the Deployment Manager process and then patch the other nodes in the cell.
- The workflow requires that an instance of IBM Installation Manager be installed on each of the target servers.

For information about prerequisites for WebSphere 8.0 or 8.5.x, refer to the [WebSphere 8 Product Documentation](#).

How this Workflow Works

The following information describes how the "WebSphere 8 - Patch Network Cell" workflow works:

Overview

This workflow installs cumulative fixes and updates for a WebSphere 8.0 or 8.5.x application server.

The workflow supports the patching of WebSphere 8.0 or 8.5.x running in a Network Deployment topology and standalone profile.

Validation Checks Performed

The validation centers on the input parameters:

- The input parameters have the proper syntax (no special characters or spaces).
- Specified files exist and have valid permissions.

Steps Executed

The WebSphere 8 - Patch Network Cell workflow includes the following steps. Each step must complete successfully before the next step can start. If a step fails, the workflow restores the configuration, cleans up files as necessary, reports a failure, and skips all subsequent steps.

Steps for WebSphere 8 - Patch Network Cell

Workflow Step	Description
Gather Parameters For WebSphere8 Network Cell Patching	Gathers the required parameters needed to patch the IBM WebSphere Application Server V8.0 and 8.5.x.
Gather Advanced Parameters For WebSphere8 Network Cell Patching	Gathers the optional parameters needed to patch the IBM WebSphere Application Server V8.0 and 8.5.x.
Get WSAAdmin Call Wrapper	Creates the necessary call wrapper to call <code>wsadmin</code> to execute certain operations within the WebSphere 8.0 or 8.5.x environment.
Validate Parameters For WebSphere8 Patching Network Cell	This step validates the basic and advanced parameters provided by the user, and checks the prerequisites for patching the IBM WebSphere Application Server.
Check File Download	Checks for the existence of a file on the target machine before downloading that file from the DMA server. For each file in the list: <ol style="list-style-type: none"> 1. The step determines whether the file is in the expected location on the target machine. 2. If the file is not in the expected location, the step adds that file to a list of files that need to be downloaded.
Download Software	Automates the transfer of files from the software repository to individual managed servers for use in downstream workflow steps.
WebSphere Backup Config	Uses the <code>backupConfig</code> utility to backup the WebSphere configurations for the specified WebSphere 8.0 or 8.5.x installation.
Verify Install Manager Exists	Verifies that an IBM Installation Manager instance exists on each of the specified target machines.
WebSphere Patching Extract Archive v2	First checks to ensure that the archive file exists. Then, based on the archive extension, extracts the archive to the specified directory.
WebSphere Stop Application Servers v2	Stops all application servers that are in started state before patching the installation of WebSphere.
WebSphere Stop Management Processes v2	First stops <code>nodeagents</code> . If there is a <code>dmgr</code> process running, the step will then stop that process before patching the WebSphere 8.0 or 8.5.x installation.
Verify All Java Processes Stopped	Verifies that all Java processes relevant to the WebSphere services on the specified target have been stopped.
WebSphere Apply Patches v2	Uses the IBM Installation Manager to apply the

Steps for WebSphere 8 - Patch Network Cell, continued

Workflow Step	Description
	cumulative patches to the specified WebSphere 8.0 or 8.5.x installation.
WebSphere Start Management Processes v2	First starts the <code>dmgr</code> process first if one exists. Then, starts the <code>nodeagent</code> process.
WebSphere Restore Config	If the patching process fails, this step is called to restore the configuration via the <code>restoreConfig</code> utility.
WebSphere Start Application Servers v2	Starts only the application servers that were stopped by the WebSphere Stop Application Servers step.
WebSphere Start Management Processes	First starts the <code>dmgr</code> process first if one exists. Then, starts the <code>nodeagent</code> process.
WebSphere Cleanup Downloaded Files	Removes all temporary downloaded files and archives.
WebSphere Start Application Servers v2	Starts only the application servers that were stopped by the WebSphere Stop Application Servers step.
Discover WebSphere	<p>Examines the target server's physical environment to discover information about WebSphere 8 cells, clusters, and managed servers.</p> <p>Note: Discovery is ONLY additive. It will not remove instances or databases currently in your environment. It is your DMA administrator's responsibility to delete content that is no longer in use.</p>

For parameter descriptions and defaults, see ["Parameters for WebSphere 8 - Patch Network Cell"](#).

How to Run this Workflow

The following instructions show you how to customize and run the ["WebSphere 8 - Patch Network Cell"](#) workflow in your environment.

Note: Before following this procedure, review the ["Prerequisites for this Workflow"](#) on page 1375, and ensure that all requirements are satisfied.

To use the Patch WebSphere 8 Network Deployment Cell workflow:

1. Create a deployable copy of the workflow.
2. Determine the values that you will specify for the following parameters:

Parameter Name	Default Value	Required	Description
Config Backup File	no default	required	Fully qualified file path where the WebSphere BackupConfig utility will write the backup file. For example: /opt/IBM/WebSphere/newbackup/backup.zip
Enable Security	true	required	Enables administrative security. Must be set to either true or false. If Enable Security is true, the WAS Admin User and WAS Admin Password parameters must have values.
WAS Admin Password	myPwd	required	If global security is enabled, this is the password for a user who belongs to a group that has permission to change the state of a specific application server.
WAS Admin User	myUsername	required	If global security is enabled, this is the user account for a user who belongs to a group that has permission to change the state of a specific application server.
WebSphere Install Location	see description	required	Fully qualified file path of the specific IBM WebSphere Application Server installation which needs to be patched. For example: /usr/IBM/WebSphere/AppServer or /opt/IBM/WebSphere/AppServer
WebSphere Patch File List	no default	required	Comma-separated list of WebSphere cumulative patch files on the target machine. For example: 8.0.0-WS-WAS-FP0000003-part1.zip, 8.0.0-WS-WAS-FP0000003-part2.zip
WebSphere Staging Location	no default	required	Fully qualified file path of the location where the list of patch files are downloaded. usr/IBM/patches/ or tmp/IBM/patches/

Tip: To avoid having to re-enter passwords whenever they change, you can create a policy to provide them to the workflow.

Note: See "[Parameters for WebSphere 8 - Patch Network Cell](#)" on page 1383 for detailed descriptions of all input parameters for this workflow, including default values.

3. In the workflow editor, expose any additional parameters that you need. You will specify values for those parameters when you create the deployment.
4. Save the changes to the workflow (click **Save** in the lower right corner).
5. Create a new deployment.
6. On the Parameters tab, specify values for the required parameters listed in step 2 and any additional parameters that you have exposed. You do not need to specify values for those parameters whose default values are appropriate for your environment.
7. On the Targets tab, specify one or more targets for this deployment.
8. Save the deployment (click **Save** in the lower right corner).
9. Run the workflow using this deployment.

To verify the results:

The workflow will complete and report SUCCESS on the Console if it has run successfully. If an error occurs during workflow execution, the error is logged, and the workflow terminates in the FAILURE state.

Sample Scenario

It is very straightforward to run the ["WebSphere 8 - Patch Network Cell"](#) workflow. This topic shows you typical parameter values to use.

For the sample use case scenario below, security is enabled.

Parameter Name	Example Value	Description
Config Backup File	no default	Fully qualified file path where the WebSphere BackupConfig utility will write the backup file. For example: /opt/IBM/WebSphere/newbackup/backup.zip
Enable Security	true	Enables administrative security. Must be set to either true or false. If Enable Security is true, the WAS Admin User and WAS Admin Password parameters must have values.
WAS Admin Password	myPwd	If global security is enabled, this is the password for a user who belongs to a group that has permission to change the state of a specific application server.
WAS Admin User	myUsername	If global security is enabled, this is the user account for a user who belongs to a group that has permission to change the state of a specific application server.
WebSphere Install Location	see description	Fully qualified file path of the specific IBM WebSphere Application Server installation which needs to be patched. For example: /usr/IBM/WebSphere/AppServer or /opt/IBM/WebSphere/AppServer
WebSphere Patch File List	no default	Comma-separated list of WebSphere cumulative patch files on the target machine. For example: 8.0.0-WS-WAS-FP0000003-part1.zip, 8.0.0-WS-WAS-FP0000003-part2.zip
WebSphere Staging Location	no default	Fully qualified file path of the location where the list of patch files are downloaded. usr/IBM/patches/ or tmp/IBM/patches/

Parameters for WebSphere 8 - Patch Network Cell

The following tables describe the required and optional input parameters for this workflow.

Parameters Defined in this Step: Gather Parameters For WebSphere8 Network Cell Patching

Parameter Name	Default Value	Required	Description
Config Backup File	no default	required	Fully qualified file path where the WebSphere BackupConfig utility will write the backup file. For example: /opt/IBM/WebSphere/newbackup/backup.zip
Enable Security	true	required	Enables administrative security. Must be set to either true or false. If Enable Security is true, the WAS Admin User and WAS Admin Password parameters must have values.
WAS Admin Password	myPwd	required	If global security is enabled, this is the password for a user who belongs to a group that has permission to change the state of a specific application server.
WAS Admin User	myUsername	required	If global security is enabled, this is the user account for a user who belongs to a group that has permission to change the state of a specific application server.
WebSphere Install Location	see description	required	Fully qualified file path of the specific IBM WebSphere Application Server installation which needs to be patched. For example: /usr/IBM/WebSphere/AppServer or /opt/IBM/WebSphere/AppServer
WebSphere Patch File List	no default	required	Comma-separated list of WebSphere cumulative patch files on the target machine. For example: 8.0.0-WS-WAS-FP0000003-part1.zip, 8.0.0-WS-WAS-FP0000003-part2.zip
WebSphere Staging Location	no default	required	Fully qualified file path of the location where the list of patch files are downloaded. usr/IBM/patches/ or tmp/IBM/patches/

IBM HTTP Server - Patch Software v2

The workflow supports the patching of IBM HTTP Server for WebSphere Application Server 8.0 or 8.5.x on the target system.

IBM HTTP Server version 8.0 or 8.5.x is a Web server that will serve both static and dynamic content. Usually you will front your WebSphere Application Server environment with an IBM HTTP Server.

To use this workflow in your environment, see the following information:

Topic	Information Included
"Prerequisites for this workflow"	List of prerequisites that must be satisfied before you can run this workflow
"How this workflow works"	Information about what the workflow does, including validation checks performed, steps executed, and a high-level process flow
"How to run this workflow "	Instructions for running this workflow in your environment
"Sample scenario"	Examples of typical parameter values for this workflow
"Parameters for IBM HTTP Server - Patch Software v2" on page 1392	List of input parameters for this workflow

Prerequisites for this workflow

Be sure that the following prerequisites are satisfied before you run this workflow:

1. You have installed the DMA AS Patching solution pack.
2. You have a valid HP Software support contract for this solution pack.
3. You have downloaded and installed all available DMA patches and hot fixes.
4. IBM Installation Manager software exists on each target machine.

For specific target operating system versions supported by each workflow, see the *Database and Middleware Automation Support Matrix*.

Dependencies:

- The workflow requires unrestricted sudo access to the user, typically root user, who can access all the required files and directories.
- The workflow requires that an instance of IBM Installation Manager be installed on each of the target servers.
- The workflow supports the patching of IHS 8.0 or 8.5.x running on a machine.

For information about prerequisites for WebSphere 8.0 or 8.5.x, refer to the [IBM HTTP Server 8.5 Product Documentation](#).

How this workflow works

The following information describes how the ["IBM HTTP Server - Patch Software v2" on page 1383](#) workflow works:

Overview

This workflow applies cumulative fixes to a specific installation of the IBM HTTP Server in an existing instance of IBM HTTP Server. It takes into account the multiple instances related to a specific installation of the IBM HTTP server and ensures all its server instances are stopped before patching.

Steps Executed

The IBM HTTP Server - Patch Software workflow includes the following steps. Each step must complete successfully before the next step can start. If a step fails, the workflow restores the configuration, cleans up files as necessary, reports a failure, and skips all subsequent steps.

Steps for IBM HTTP Server - Patch Software

Workflow Step	Description
Gather Parameters for IBM HTTP Server - Patch Software	Gathers the required parameters needed to patch the IBM HTTP Server V8.0 and 8.5.x.
Gather Advanced Parameters for IBM HTTP Server - Patch Software	Gathers the optional parameters needed to patch the IBM HTTP Server V8.0 and 8.5.x.
Validate Parameters for IBM HTTP Server - Patch Software	This step validates the basic and advanced parameters provided by the user, and checks the prerequisites for patching the IBM HTTP Server.
Check File Download	Checks for the existence of a file on the target machine before downloading that file from the DMA server. For each file in the list: <ol style="list-style-type: none"> 1. The step determines whether the file is in the expected location on the target machine. 2. If the file is not in the expected location, the step adds that file to a list of files that need to be downloaded.
Download Software	Automates the transfer of files from the software repository to individual managed servers for use in downstream workflow steps.
Verify Install Manager Exists	Verifies that an IBM Installation Manager instance exists on each of the specified target machines.
WebSphere Patching Extract Archive v2	First checks to ensure that the archive file exists. Then, based on the archive extension, extracts the archive to the specified directory.
IBM HTTP Server Stop Application Servers v2	Stops all application servers that are in started state.
Verify All IHS Processes Stopped	Verifies validates that all server instances on a given machine have been stopped.
IBM HTTP Server Apply Patch	Utilizes the WebSphere Install Manager to apply the cumulative patches to a given HTTP Server installation.
IBM HTTP Server Start Application Servers	Checks the state of each application server, and starts only the application servers that were stopped by the IBM - HTTPServer Stop Application Server step.
IBM HTTP Server Start Application Servers	Checks the state of each application server, and starts only the application servers that were stopped by the IBM - HTTPServer Stop Application Server step.
Discover IBM HTTP Server	Audits the server's physical environment looking for IBM HTTP Server instances.

Steps for IBM HTTP Server - Patch Software, continued

Workflow Step	Description
	Note: Discovery is ONLY additive. It will not remove instances or databases currently in your environment. It is your DMA administrator's responsibility to delete content that is no longer in use.
Cleanup Downloaded Files	Removes all downloaded files and archives.

For parameter descriptions and defaults, see ["Parameters for IBM HTTP Server - Patch Software v2"](#)

How to run this workflow

The following instructions show you how to customize and run the ["IBM HTTP Server - Patch Software v2" on page 1383](#) workflow in your environment.

Note: Before following this procedure, review the ["Prerequisites for this workflow" on page 1385](#), and ensure that all requirements are satisfied.

To use the IBM HTTP Server - Patch Software workflow:

1. Create a deployable copy of the workflow.
2. Determine the values that you will specify for the following parameters: show

Parameter Name	Default Value	Required	Description
IHS Install Location	no default	required	Fully qualified directory path of the specific IBM HTTP Server installation which needs to be patched.
IHS Patch File List	no default	required	Comma separated list of patch files to be patched. For example: 8.0.0-WS-WAS-FP0000003-part1.zip, 8.0.0-WS-WAS-FP0000003-part2.zip
Staging Location	no default	required	The list of patch files that are downloaded.

Tip: To avoid having to re-enter passwords whenever they change, you can create a policy to provide them to the workflow.

Note: See ["Parameters for IBM HTTP Server - Patch Software v2" on page 1392](#) for detailed descriptions of all input parameters for this workflow, including default values.

3. In the workflow editor, expose any additional parameters that you need. You will specify values for those parameters when you create the deployment.
4. Save the changes to the workflow (click **Save** in the lower right corner).
5. Create a new deployment.
6. On the Parameters tab, specify values for the required parameters listed in step 2 and any additional parameters that you have exposed. You do not need to specify values for those parameters whose default values are appropriate for your environment.
7. On the Targets tab, specify one or more targets for this deployment.

8. Save the deployment (click **Save** in the lower right corner).
9. Run the workflow using this deployment.

To verify the results:

The workflow will complete and report SUCCESS on the Console if it has run successfully. If an error occurs during workflow execution, the error is logged, and the workflow terminates in the FAILURE state.

Parameters for IBM HTTP Server - Patch Software v2

The following tables describe the required and optional input parameters for this workflow.

Parameters Defined in this Step: Gather Parameters For IBM HTTP Server - Patch Software v2

Parameter Name	Default Value	Required	Description
IHS Install Location	no default	required	Fully qualified directory path of the specific IBM HTTP Server installation which needs to be patched.
IHS Patch File List	no default	required	Comma separated list of patch files to be patched. For example: 8.0.0-WS-WAS-FP0000003-part1.zip, 8.0.0-WS-WAS-FP0000003-part2.zip
Staging Location	no default	required	The list of patch files that are downloaded.

Sample scenario

It is very straightforward to run the ["IBM HTTP Server - Patch Software v2" on page 1383](#) workflow. This topic shows you typical parameter values to use.

For the sample use case scenario below, security is enabled.

Parameter Name	Example Value	Description
IHS Install Location	no default	Fully qualified directory path of the specific IBM HTTP Server installation which needs to be patched.
IHS Patch File List	no default	Comma separated list of patch files to be patched. For example: 8.0.0-WAS-WAS-FP0000003-part1.zip, 8.0.0-WAS-WAS-FP0000003-part2.zip
Staging Location	no default	The list of patch files that are downloaded.

WebSphere - Provision WebSphere SDK Java

This workflow installs IBM Java SDK for WebSphere Application Server and enables all the profiles of WebSphere Application Server to use the new version of Java.

The workflow takes into account the multiple instances or profiles related to a specific installation of the IBM WebSphere Application server and ensures all its components (dmgr, nodeagent and application servers) are stopped before enabling the SDK.

To use this workflow in your environment, see the following information:

Topic	Information Included
"Prerequisites for this workflow"	List of prerequisites that must be satisfied before you can run this workflow
"How this workflow works"	Information about what the workflow does, including validation checks performed, steps executed, and a high-level process flow
"How to run this workflow "	Instructions for running this workflow in your environment
"Sample scenario"	Examples of typical parameter values for this workflow
"Parameters for WebSphere - Provision WebSphere SDK Java" on page 1401	List of input parameters for this workflow

Prerequisites for this workflow

Ensure that the following prerequisites are satisfied before you run this workflow:

1. You have installed the DMA ASProvisioning solution pack.
2. You have a valid HP Software support contract for this solution pack.
3. You have downloaded and installed all available DMA patches and hot fixes.
4. IBM Installation Manager software exists on each target machine.

For specific target operating system versions supported by each workflow, see the *Database and Middleware Automation Support Matrix* available on the Software Support web site:

<https://softwaresupport.hp.com/>

Dependencies:

- The workflow requires unrestricted `sudo` access to the user, typically root user, who can access all the required files and directories.
- The workflow requires that an instance of IBM Installation Manager be installed on each of the target servers.
- The workflow requires that an instance of the WebSphere Application Server be installed on the target machine.

For information about prerequisites for WebSphere Java SDK, refer to the [IBM WebSphere Java SDK Product Documentation](#).

How this workflow works

The following information describes how the ["WebSphere - Provision WebSphere SDK Java" on page 1393](#) workflow works:

Overview

This workflow installs IBM Java SDK for WebSphere Application Server and enables all the profiles of WebSphere Application Server to use the new version of Java. It takes into account the multiple instances or profiles related to a specific installation of the IBM WebSphere Application Server and ensures all its components (dmgr, nodeagent and application servers) are stopped before enabling the SDK.

Steps Executed

The WebSphere - Provision WebSphere SDK Java workflow includes the following steps. Each step must complete successfully before the next step can start. If a step fails, the workflow restores the configuration, cleans up files as necessary, reports a failure, and skips all subsequent steps.

Steps for WebSphere - Provision WebSphere SDK Java

Workflow Step	Description
Gather Parameters for WebSphere - Provision WebSphere SDK Java	Gathers the required parameters needed to provision the IBM Java SDK of WebSphere Application Server.
Gather Advanced Parameters for WebSphere - Provision WebSphere SDK Java	Gathers the optional parameters needed to provision the IBM Java SDK of WebSphere Application Server.
Get WSAAdmin Call Wrapper	This step creates the necessary call wrapper to call wsadmin to execute certain operations within a given WebSphere environment.
Validate Parameters for WebSphere - Provision WebSphere SDK Java	This step validates the basic and advanced parameters provided by the user, and checks the prerequisites for provisioning the IBM WebSphere Application Server.
Check File Download	Checks for the existence of a file on the target machine before downloading that file from the DMA server. For each file in the list: <ol style="list-style-type: none"> 1. The step determines whether the file is in the expected location on the target machine. 2. If the file is not in the expected location, the step adds that file to a list of files that need to be downloaded.
Download Software	Automates the transfer of files from the software repository to individual managed servers for use in downstream workflow steps.
Verify Install Manager Exists	Verifies that an IBM Installation Manager instance exists on a given target machine.
WebSphere 8 Patching Extract Archive V2	First checks to ensure that the archive file exists. Then, based on the archive extension, extracts the archive to the specified directory.
WebSphere Stop Application Servers V2	This step takes a list of WebSphere Application Servers, checks the state of each application server, and stops only the application servers that are in the started state.
WebSphere 8 Stop Management Processes V2	This step stops the Nodeagents and the dmgr process that is running before provisioning the installation of WebSphere.
Verify All Java Processes Stopped	This step validates that all Java processes on a given machine have been stopped.
Provision WebSphere SDK Java	This step utilizes the WebSphere Install Manager to provision SDK to a given WebSphere installation.
WebSphere 8 Start Management Processes V2	This step starts the dmgr process first, if a dmgr process exists and then starts the Nodeagent process.

Steps for WebSphere - Provision WebSphere SDK Java, continued

Workflow Step	Description
WebSphere Start Application Servers V2	This step takes a list of WebSphere Application Servers, checks the state of each application server, and starts only the application servers that were stopped by the WebSphere Stop Application Servers step.
Enable Profiles - Provision WebSphere SDK Java	This step utilizes the WebSphere Install Manager to provision SDK to a given WebSphere installation.
WebSphere Start Application Servers and Restart Node agent	This step takes a list of WebSphere Application Servers, checks the state of each application server, and starts only the application servers that were stopped by the WebSphere Stop Application Servers step, and the Node Agents.
Discover WebSphere	<p>Audits the server's physical environment looking for IBM WebSphere Application Server instances.</p> <p>Note: Discovery is ONLY additive. It will not remove instances or databases currently in your environment. It is your DMA administrator's responsibility to delete content that is no longer in use.</p>
Cleanup Downloaded Files	Removes all downloaded files and archives.

For parameter descriptions and defaults, see ["Parameters for WebSphere - Provision WebSphere SDK Java"](#).

How to run this workflow

The following instructions show you how to customize and run the ["WebSphere - Provision WebSphere SDK Java" on page 1393](#) workflow in your environment.

Note: Before following this procedure, review the ["Prerequisites for this workflow" on page 1394](#), and ensure that all requirements are satisfied.

To use the WebSphere - Provision WebSphere SDK Java workflow:

1. Create a deployable copy of the workflow.
2. Determine the values that you will specify for the following parameters:

Parameter Name	Default Value	Required	Description
Enable Security	no default	required	Enables administrative security. Must be set to either true or false. If Enable Security is true, the WAS Admin User and WAS Admin Password parameters must have values.
WAS Admin Password	no default	required	If global security is enabled, this is the password for a user who belongs to a group that has permission to change the state of a specific application server.
WAS Admin User	no default	required	If global security is enabled, this is the user account for a user who belongs to a group that has permission to change the state of a specific application server.
WebSphere Install Location	no default	required	Fully qualified file path of the specific IBM WebSphere Application Server installation where SDK needs to be provisioned.
WebSphere SDK File List	no default	required	Comma separated list of files for provisioning on the target machine. Example: WS_SDK_JAVA_TEV7.0_1OF3_WAS_8.5.5.zip,WS_SDK_JAVA_TEV7.0_2OF3_WAS_8.5.5.zip,WS_SDK_JAVA_TEV7.0_3OF3_WAS_8.5.5.zip
WebSphere Staging Location	no default	required	Fully qualified file path of the location where the list of files are downloaded. Example: usr/IBM/ and tmp/IBM

Tip: To avoid having to re-enter passwords whenever they change, you can create a policy to provide them to the workflow.

Note: See ["Parameters for WebSphere - Provision WebSphere SDK Java" on page 1401](#) for detailed descriptions of all input parameters for this workflow, including default values.

3. In the workflow editor, expose any additional parameters that you need. You will specify values for those parameters when you create the deployment.

4. Save the changes to the workflow (click **Save** in the lower right corner).
5. Create a new deployment.
6. On the Parameters tab, specify values for the required parameters listed in step 2 and any additional parameters that you have exposed. You do not need to specify values for those parameters whose default values are appropriate for your environment.
7. On the Targets tab, specify one or more targets for this deployment.
8. Save the deployment (click **Save** in the lower right corner).
9. Run the workflow using this deployment.

To verify the results:

The workflow will complete and report SUCCESS on the Console if it has run successfully. If an error occurs during workflow execution, the error is logged, and the workflow terminates in the FAILURE state.

Parameters for WebSphere - Provision WebSphere SDK Java

The following tables describe the required and optional input parameters for this workflow.

Parameters Defined in this Step: Gather Parameters for Provision WebSphere SDK Java

Parameter Name	Default Value	Required	Description
Enable Security	no default	required	Enables administrative security. Must be set to either true or false. If Enable Security is true, the WAS Admin User and WAS Admin Password parameters must have values.
WAS Admin Password	no default	required	If global security is enabled, this is the password for a user who belongs to a group that has permission to change the state of a specific application server.
WAS Admin User	no default	required	If global security is enabled, this is the user account for a user who belongs to a group that has permission to change the state of a specific application server.
WebSphere Install Location	no default	required	Fully qualified file path of the specific IBM WebSphere Application Server installation where SDK needs to be provisioned.
WebSphere SDK File List	no default	required	Comma separated list of files for provisioning on the target machine. Example: WS_SDK_JAVA_TEV7.0_1OF3_WAS_8.5.5.zip,WS_SDK_JAVA_TEV7.0_2OF3_WAS_8.5.5.zip,WS_SDK_JAVA_TEV7.0_3OF3_WAS_8.5.5.zip
WebSphere Staging Location	no default	required	Fully qualified file path of the location where the list of files are downloaded.

Sample scenario

It is very straightforward to run the ["WebSphere - Provision WebSphere SDK Java" on page 1393](#) workflow. This topic shows you typical parameter values to use.

For the sample use case scenario below, security is enabled.

Parameter Name	Example Value	Description
Enable Security	no default	Enables administrative security. Must be set to either true or false. If Enable Security is true, the WAS Admin User and WAS Admin Password parameters must have values.
WAS Admin Password	no default	If global security is enabled, this is the password for a user who belongs to a group that has permission to change the state of a specific application server.
WAS Admin User	no default	If global security is enabled, this is the user account for a user who belongs to a group that has permission to change the state of a specific application server.
WebSphere Install Location	no default	Fully qualified file path of the specific IBM WebSphere Application Server installation where SDK needs to be provisioned.
WebSphere SDK File List	no default	Comma separated list of files for provisioning on the target machine. Example: WS_SDK_JAVA_TEV7.0_1OF3_WAS_8.5.5.zip,WS_SDK_JAVA_TEV7.0_2OF3_WAS_8.5.5.zip,WS_SDK_JAVA_TEV7.0_3OF3_WAS_8.5.5.zip
WebSphere Staging Location	no default	Fully qualified file path of the location where the list of files are downloaded.

Configure WebSphere Cluster and Cluster Members

The purpose of this workflow is to create a new WebSphere Application Server cluster, create cluster members, and configure each cluster member.

The cluster members can be both vertically and horizontally clustered depending on the number of cluster members specified and the number of nodes that are within a cell.

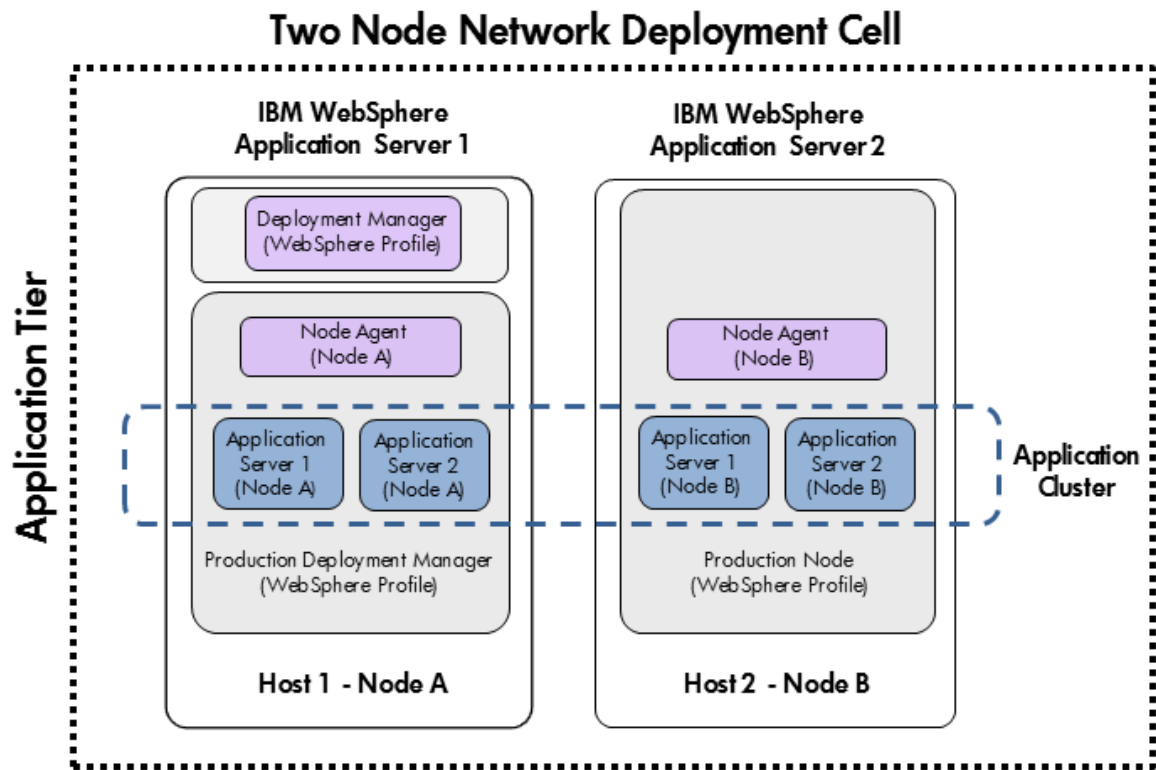
The cluster members are configured consistently based on a set of configurable parameters. If you do not specify parameters then the default WebSphere values are used.

The following chart shows the customizable parameters for WebSphere clusters and cluster members:

Cluster/cluster member attribute	Configurable parameter
Cluster definition	Cluster Name Cluster Member Name Number Cluster Members
Java Virtual Machine (JVM)	Initial Heap Size Maximum Heap Size
Logging	Logfile Location Rollover Type (SIZE, TIME, NONE, or BOTH) Base Hour Rollover Period Rollover Size Maximum Rollback Files

Architecture Diagram

The following is an example of a WebSphere Application Server environment:



To use this workflow in your environment, see the following information:

Topic	Information Included
"Prerequisites for this Workflow"	List of prerequisites that must be satisfied before you can run this workflow
"How this Workflow Works"	Information about what the workflow does, including validation checks performed, steps executed, and a high-level process flow
"How to Run this Workflow"	Instructions for running this workflow in your environment
"Sample Scenario"	Examples of typical parameter values for this workflow
Parameters	List of input parameters for this workflow

Prerequisites for this Workflow

Be sure that the following prerequisites are satisfied before you run the Configure WebSphere Cluster and Cluster Members workflow.

Product Platform

This workflow is available for WebSphere7.0, 8.0, or 8.5.x.

Dependencies

This workflow has the following dependencies:

- You must have a working WebSphere Network Deployment cell version 7.0, 8.0, or 8.5.x, with the Deployment Manager available for communication.
- You must run the Discover WebSphere workflow before you run the workflows. The Discover WebSphere workflow audits the server's physical environment for WebSphere cells, clusters, and application servers and stores the configuration information in the DMA environment.

For more information about prerequisites for WebSphere, refer to the [WebSphere 8 Product Documentation](#).

How this Workflow Works

The following information describes how the Configure WebSphere Cluster and Cluster Members workflow works:

Overview

This workflow does the following things in the order shown:

1. Before creating the cluster and cluster members, the workflow prepares and validates all parameters and creates the call wrapper that will be used to execute commands within a WebSphere environment.
2. Next the workflow uses the call wrapper to call `wsadmin` to create the cluster and cluster members and to configure the cluster members.
3. Then the workflow starts the cluster to verify that it starts correctly and calls the component workflow, Discover WebSphere, to look for WebSphere configurations—including clusters and cluster members attributes.

Validation Checks Performed

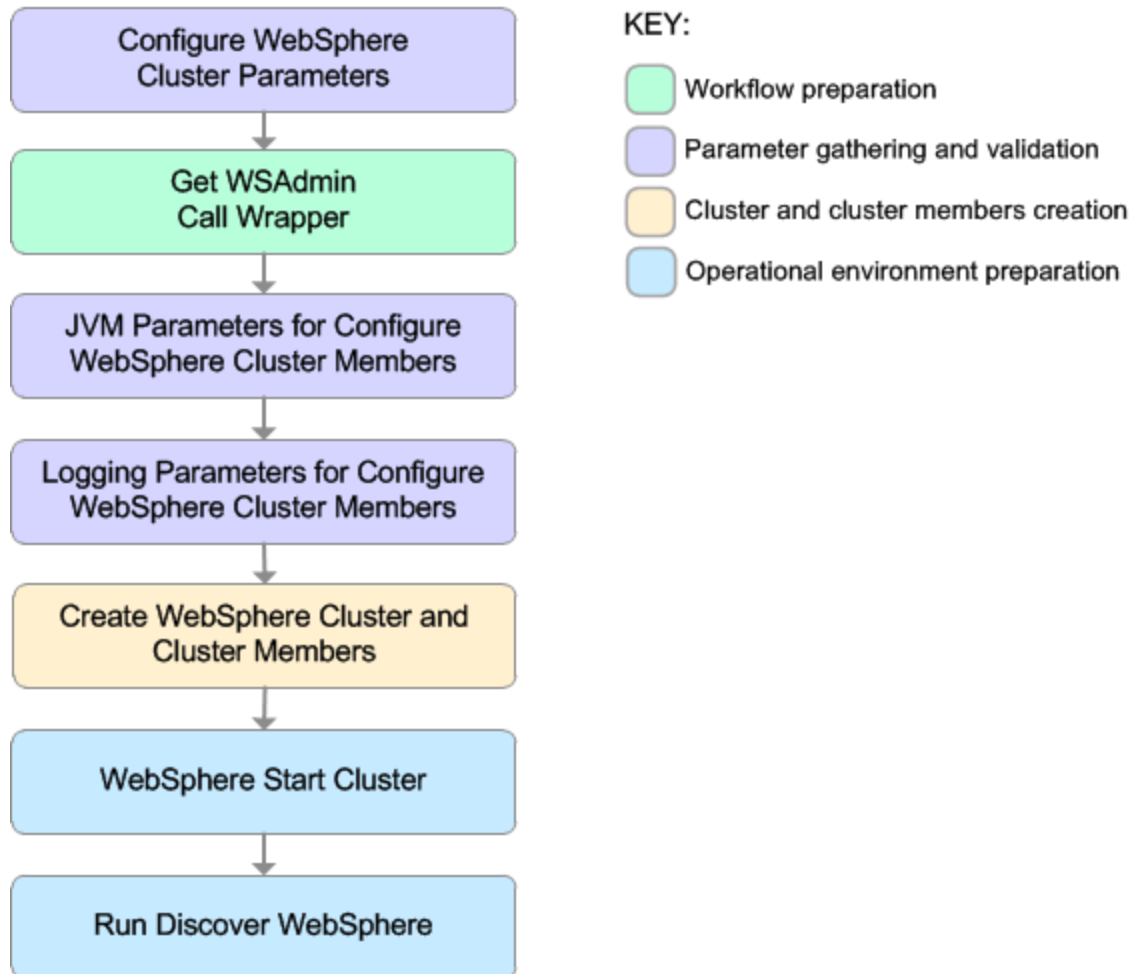
The workflow then performs the following checks on the input parameters:

WebSphere Admin Username	Cannot contain the following characters <code>/ \ * , ; = + ? < > & % ' " [] # \$ ^ { }</code> and also cannot begin with a dash (-), period (.), or space ()
WebSphere Admin Password	Cannot begin with a dash (-) and cannot contain a space ()
Cluster Name Cluster Member Name	Must be specified Cannot contain the following characters <code>/ \ * , ; = + ? < > & % ' " [] # \$ ^ { }</code> or space Cannot begin with a period (.)
Enable Security	Must be true or false
If Enable Security is true	WebSphere Admin Username must be specified WebSphere Admin Password must be specified
Number Cluster Members	If specified, must be an integer
Web Service URL Web Service User Web Service Password Cluster Name Cluster Member Name	Must be specified
WebSphere Home WebSphere Dmgr Port	Must be found in the metadata

WebSphere Dmgr Host	
Initial Heap Size Maximum Heap Size	If one is specified the other must also be specified If specified, must be non-negative integers with an optional leading plus sign (+) If specified, Maximum Heap Size must be greater than Initial Heap Size
Rollover Type	Must be BOTH, SIZE, NONE, or TIME (case dependent)
If Rollover Type is either BOTH or SIZE	Rollover Size must be specified
Maximum Rollback Files Rollover Size	If specified, must be non-negative integers with an optional leading plus sign (+)
Base Hour Rollover Period	If specified, must be integers between 1 and 24
Logfile Location	Must be a valid fully-qualified directory path that exists or can be created.
Web Service Password Web Service URL Web Service User	Must define a valid WebSphere Home

Steps Executed

The Configure WebSphere Cluster and Cluster Members workflow includes the following steps. Each step must complete successfully before the next step can start. If a step fails, the workflow reports a failure and all subsequent steps are skipped.



Steps Used in the Configure WebSphere Cluster and Cluster Members Workflow

Workflow Step	Description
Configure WebSphere Cluster Parameters	This step prepares and validates the parameters needed to create a cluster and cluster members for WebSphere Application Server. This step also prepares the parameters needed for the <code>wsadmin</code> call wrapper.
Get WSAdmin Call Wrapper	This step creates the necessary call wrapper to call <code>wsadmin</code> to execute certain operations within a given WebSphere environment.
JVM Parameters for Configure WebSphere Cluster Members	This step prepares and validates the parameters needed to configure Java Virtual Machine (JVM) parameters for each of the newly created WebSphere Application Server cluster members.
Logging Parameters for Configure WebSphere Cluster Members	This step prepares and validates the parameters needed to configure logging parameters for each of the newly created WebSphere Application Server cluster members.
Create WebSphere Cluster and Cluster Members	This step creates a new WebSphere Application Server cluster and cluster members. It also configures any of the cluster members with the optional configurations.
WebSphere Start Cluster	This step starts the newly created WebSphere Application Server cluster and cluster members and then checks the status of the cluster to make

Steps Used in the Configure WebSphere Cluster and Cluster Members Workflow, continued

Workflow Step	Description
	sure it started correctly.
Run Discover WebSphere	<p>This step runs Discover WebSphere to examines the target server's physical environment to discover information about WebSphere cells, clusters, and application servers.</p> <p>Note: Discovery is ONLY additive. It will not remove instances or databases currently in your environment. It is your DMA administrator's responsibility to delete content that is no longer in use.</p>

For parameter descriptions and defaults, see ["Parameters for Configure WebSphere Cluster and Cluster Members" on page 1422](#).

How to Run this Workflow

The following instructions show you how to customize and run the Configure WebSphere Cluster and Cluster Members workflow in your environment.

The workflow provides default values for some parameters. These default values are usually sufficient for a "typical" installation. You can override the defaults by specifying parameter values in the deployment. You can also expose additional parameters in the workflow, if necessary, to accomplish more advanced scenarios. Any parameters not explicitly specified in the deployment will have the default values listed in ["Parameters for Configure WebSphere Cluster and Cluster Members" on page 1422](#).

Note: Before following this procedure, review the ["Prerequisites for this Workflow"](#), and ensure that all requirements are satisfied.

To use the Configure WebSphere Cluster and Cluster Members workflow:

1. Create a deployable copy of the workflow.
2. Determine the values that you will specify for the following parameters:

Input Parameters for Configure WebSphere Cluster Parameters

Parameter Name	Default Value	Required	Description
Cluster Member Name	no default	required	The base cluster member name that will be used for each cluster member/application server. A suffix will automatically be appended to this base name that will indicate the node and cluster. For the initial cluster, the suffixes will be 001a for the first node, 001b for second node, and so on. If a vertical cluster member is created, the suffixes will be 002a for the first node, 002b for the second node, and so on. It cannot contain any of the following characters / \ * , ; = + ? < > & % ' " [] # \$ ^ { }.
Cluster Name	no default	required	This is the name given to the logical grouping of cluster members. This name has to be unique to the cell. It cannot contain any of the following characters / \ * , ; = + ? < > & % ' " [] # \$ ^ { }.
Enable Security	no default	required	Indicates whether security will be enabled. Valid values are True or False. If True then WebSphere Admin Password and WebSphere Admin User must have values.

Input Parameters for Configure WebSphere Cluster Parameters, continued

Parameter Name	Default Value	Required	Description
Number Cluster Members	no default	required	The number of cluster members/application servers that will be created on each node.
Web Service Password	no default	required	Password for the DMA Discovery web service API.
Web Service URL	no default	required	URL for the DMA Discovery web service API. For example: <code>https://example.com:8443/dma</code>
Web Service User	no default	required	A user capable of modifying the DMA managed environment by using the web service API.
WebSphere Admin Password	no default	optional	The password for a user in a group that can change the state of a given application server. Only required if global security is enabled. It cannot begin with a dash (-) or contain a space ().
WebSphere Admin Username	no default	optional	The user account for a user in a group that can change the state of a given application server. Only required if global security is enabled. It cannot begin with a dash (-), a period (.), or a space (). It cannot contain any of the following characters / \ * , ; = + ? < > & % ' " [] # \$ ^ { }.

Tip: To avoid having to re-enter passwords whenever they change, you can create a policy to provide them to the workflow.

Note: This is the minimum set of parameters required to run this workflow. You may need to expose additional parameters depending on your objectives.

See ["Parameters for Configure WebSphere Cluster and Cluster Members" on page 1422](#) for detailed descriptions of all input parameters for this workflow, including default values.

3. In the workflow editor, expose any additional parameters that you need. You will specify values for those parameters when you create the deployment
4. Save the changes to the workflow (click **Save** in the lower right corner).
5. Create a new deployment.
6. On the Parameters tab, specify values for the required parameters listed in step 2 and any

additional parameters that you have exposed. You do not need to specify values for those parameters whose default values are appropriate for your environment.

7. On the Targets tab, specify one or more targets for this deployment.
8. Save the deployment (click **Save** in the lower right corner).
9. Run the workflow using this deployment.

To verify the results:

The workflow will complete and report SUCCESS on the Console if it has run successfully. If an error occurs during workflow execution, the error is logged, and the workflow terminates in the FAILURE state.

Sample Scenario

This topic shows you typical parameter values for different use cases for the Configure WebSphere Cluster and Cluster Members workflow. For a complete list of all parameters used in this workflow, including default values, see ["Parameters for Configure WebSphere Cluster and Cluster Members" on page 1422](#).

Tip: To avoid having to re-enter passwords whenever they change, you can create a policy to provide them to the workflow.

Scenario 1: To create two cluster members on each node using the default configurations

This use case will create a cluster testCluster with two nodes testApp001a and testApp001b. Security will be enabled. The WebSphere default values will be used for Initial Heap Size, Maximum Heap Size, and for logging.

Input Parameters for Configure WebSphere Cluster Parameters

Parameter Name	Example Value	Description
Cluster Member Name	testApp	The base cluster member name that will be used for each cluster member/application server. A suffix will automatically be appended to this base name that will indicate the node and cluster. For the initial cluster, the suffixes will be 001a for the first node, 001b for second node, and so on. If a vertical cluster member is created, the suffixes will be 002a for the first node, 002b for the second node, and so on. It cannot contain any of the following characters / \ * , ; : = + ? < > & % ' " [] # \$ ^ { }.
Cluster Name	testCluster	This is the name given to the logical grouping of cluster members. This name has to be unique to the cell. It cannot contain any of the following characters / \ * , ; : = + ? < > & % ' " [] # \$ ^ { }.
Enable Security	True	Indicates whether security will be enabled. Valid values are True or False. If True then WebSphere Admin Password and WebSphere Admin User must have values.
Number Cluster Members	2	The number of cluster members/application servers that will be created on each node.
Web Service Password	myWebSvcPwd	Password for the DMA Discovery web service API.
Web Service URL	see description	URL for the DMA Discovery web service API. For example: https://example.com:8443/dma
Web Service User	JohnDoe	A user capable of modifying the DMA managed environment by using the web service API.
WebSphere Admin	myPwd	The password for a user in a group that can change the state of a given application server. Only required if global

Input Parameters for Configure WebSphere Cluster Parameters, continued

Parameter Name	Example Value	Description
Password		security is enabled. It cannot not begin with a dash (-) or contain a space ().
WebSphere Admin Username	wasadmin	The user account for a user in a group that can change the state of a given application server. Only required if global security is enabled. It cannot begin with a dash (-), a period (.), or a space (). It cannot contain any of the following characters / \ * , : ; = + ? < > & % ' " [] # \$ ^ { }.

Scenario 2: To create two cluster members on each node, specifying initial and maximum heap sizes, and using the default logging configurations

This use case will create a cluster testCluster with two nodes testApp001a and testApp001b. Security will be enabled. The Initial Heap Size will be set to 512MB and the Maximum Heap Size to 1024MB. The WebSphere default values will be used for logging.

Note: Some of these parameters are not exposed by default in the deployment. You need to expose the following:

In the step JVM Parameters for Configure WebSphere Cluster Members:

- Initial Heap Size
- Maximum Heap Size

Input Parameters for Configure WebSphere Cluster Parameters

Parameter Name	Example Value	Description
Cluster Member Name	testApp	The base cluster member name that will be used for each cluster member/application server. A suffix will automatically be appended to this base name that will indicate the node and cluster. For the initial cluster, the suffixes will be 001a for the first node, 001b for second node, and so on. If a vertical cluster member is created, the suffixes will be 002a for the first node, 002b for the second node, and so on. It cannot contain any of the following characters / \ * , ; : = + ? < > & % ' " [] # \$ ^ { }.
Cluster Name	testCluster	This is the name given to the logical grouping of cluster members. This name has to be unique to the cell. It cannot contain any of the following characters / \ * , ; : = + ? < > & % ' " [] # \$ ^ { }.
Enable Security	True	Indicates whether security will be enabled. Valid values are True or False. If True then WebSphere Admin Password and WebSphere Admin User must have values.
Number Cluster Members	2	The number of cluster members/application servers that will be created on each node.
Web Service Password	myWebSvcPwd	Password for the DMA Discovery web service API.
Web Service URL	see description	URL for the DMA Discovery web service API. For example: https://example.com:8443/dma
Web Service User	JohnDoe	A user capable of modifying the DMA managed environment by using the web service API.
WebSphere Admin Password	myPwd	The password for a user in a group that can change the state of a given application server. Only required if global security is enabled. It cannot not begin with a dash (-) or contain a space ().

Input Parameters for Configure WebSphere Cluster Parameters, continued

Parameter Name	Example Value	Description
WebSphere Admin Username	wasadmin	The user account for a user in a group that can change the state of a given application server. Only required if global security is enabled. It cannot begin with a dash (-), a period (.), or a space (.). It cannot contain any of the following characters / \ * , ; = + ? < > & % ' " [] # \$ ^ { }.

Input Parameters for JVM Parameters for Configure WebSphere Cluster Members

Parameter Name	Example Value	Description
Initial Heap Size	512	Initial heap size, in megabytes, that all cluster members will be set to on creation. The default is the WebSphere default value.
Maximum Heap Size	1024	Maximum heap size, in megabytes, that all cluster members will be set to on creation. The default is the WebSphere default value.

Scenario 3: To create two cluster members on each node, specifying initial and maximum heap sizes, and using a time-based logging configuration

This use case will create a cluster testCluster with two nodes testApp001a and testApp001b. The Initial Heap Size will be set to 512MB and the Maximum Heap Size to 1024MB. Security will not be enabled. The WebSphere periodic rollover logging will start at hour 1 (midnight), will update every 24 hours, and 7 historic logs will be saved.

Note: Some of these parameters are not exposed by default in the deployment. You need to expose the following:

In the step JVM Parameters for Configure WebSphere Cluster Members:

- Initial Heap Size
- Maximum Heap Size

In the step Logging Parameters for Configure WebSphere Cluster Members:

- Base Hour
- Logfile Location
- Maximum Rollback Files
- Rollover Period
- Rollover Type

Input Parameters for Configure WebSphere Cluster Parameters

Parameter Name	Example Value	Description
Cluster Member Name	testApp	The base cluster member name that will be used for each cluster member/application server. A suffix will automatically be appended to this base name that will indicate the node and cluster. For the initial cluster, the suffixes will be 001a for the first node, 001b for second node, and so on. If a vertical cluster member is created, the suffixes will be 002a for the first node, 002b for the second node, and so on. It cannot contain any of the following characters / \ * , ; = + ? < > & % ' " [] # \$ ^ { }.
Cluster Name	testCluster	This is the name given to the logical grouping of cluster members. This name has to be unique to the cell. It cannot contain any of the following characters / \ * , ; = + ? < > & % ' " [] # \$ ^ { }.
Enable Security	False	Indicates whether security will be enabled. Valid values are True or False. If True then WebSphere Admin Password and WebSphere Admin User must have values.
Number Cluster Members	2	The number of cluster members/application servers that will be created on each node.

Input Parameters for Configure WebSphere Cluster Parameters, continued

Parameter Name	Example Value	Description
Web Service Password	myWebSvcPwd	Password for the DMA Discovery web service API.
Web Service URL	see description	URL for the DMA Discovery web service API. For example: <code>https://example.com:8443/dma</code>
Web Service User	JohnDoe	A user capable of modifying the DMA managed environment by using the web service API.

Input Parameters for JVM Parameters for Configure WebSphere Cluster Members

Parameter Name	Example Value	Description
Initial Heap Size	512	Initial heap size, in megabytes, that all cluster members will be set to on creation. The default is the WebSphere default value.
Maximum Heap Size	1024	Maximum heap size, in megabytes, that all cluster members will be set to on creation. The default is the WebSphere default value.

Input Parameters for Logging Parameters for Configure WebSphere Cluster Members

Parameter Name	Example Value	Description
Base Hour	1	The hour of the day, from 1 to 24, when the periodic rollover starts. The rollover always starts at the specified hour of the day. Hour 1 is 00:00:00 (midnight) and hour 24 is 23:00:00. Once started, the rollover repeats every Rollover Period hours.
Logfile Location	see description	Fully qualified directory path where the SystemOut and SystemErr logs will be created. For example: <code>/app/logs</code>
Maximum Rollback Files	7	The number of historical logs to keep.
Rollover Period	24	The number of hours after which the log file rolls over. Valid values range from 1 to 24. Only used if Rollover Type is TIME or BOTH.
Rollover Type	TIME	Type of log rollover. Valid values are SIZE, TIME, NONE or BOTH. The default is SIZE.

Scenario 4: To create two cluster members on each node, specifying initial and maximum heap sizes, and using a size-based logging configuration

This use case will create a cluster testCluster with two nodes testApp001a and testApp001b. Security will not be enabled. The Initial Heap Size will be set to 512MB and the Maximum Heap Size to 1024MB. The WebSphere periodic logging will rollover when the file size reaches 100MB and 7 historic logs will be saved.

Note: Some of these parameters are not exposed by default in the deployment. You need to expose the following:

In the step JVM Parameters for Configure WebSphere Cluster Members:

- Initial Heap Size
- Maximum Heap Size

In the step Logging Parameters for Configure WebSphere Cluster Members:

- Logfile Location
- Maximum Rollback Files
- Rollover Size
- Rollover Type

Input Parameters for Configure WebSphere Cluster Parameters

Parameter Name	Example Value	Description
Cluster Member Name	testApp	The base cluster member name that will be used for each cluster member/application server. A suffix will automatically be appended to this base name that will indicate the node and cluster. For the initial cluster, the suffixes will be 001a for the first node, 001b for second node, and so on. If a vertical cluster member is created, the suffixes will be 002a for the first node, 002b for the second node, and so on. It cannot contain any of the following characters / \ * , ; = + ? < > & % ' " [] # \$ ^ { }.
Cluster Name	testCluster	This is the name given to the logical grouping of cluster members. This name has to be unique to the cell. It cannot contain any of the following characters / \ * , ; = + ? < > & % ' " [] # \$ ^ { }.
Enable Security	False	Indicates whether security will be enabled. Valid values are True or False. If True then WebSphere Admin Password and WebSphere Admin User must have values.
Number Cluster Members	2	The number of cluster members/application servers that will be created on each node.

Input Parameters for Configure WebSphere Cluster Parameters, continued

Parameter Name	Example Value	Description
Web Service Password	myWebSvcPwd	Password for the DMA Discovery web service API.
Web Service URL	see description	URL for the DMA Discovery web service API. For example: <code>https://example.com:8443/dma</code>
Web Service User	JohnDoe	A user capable of modifying the DMA managed environment by using the web service API.

Input Parameters for JVM Parameters for Configure WebSphere Cluster Members

Parameter Name	Example Value	Description
Initial Heap Size	512	Initial heap size, in megabytes, that all cluster members will be set to on creation. The default is the WebSphere default value.
Maximum Heap Size	1024	Maximum heap size, in megabytes, that all cluster members will be set to on creation. The default is the WebSphere default value.

Input Parameters for Logging Parameters for Configure WebSphere Cluster Members

Parameter Name	Example Value	Description
Logfile Location	see description	Fully qualified directory path where the SystemOut and SystemErr logs will be created. For example: <code>/app/logs</code>
Maximum Rollback Files	7	The number of historical logs to keep.
Rollover Size	100	The maximum size of the log file in megabytes. When the file reaches this size, it rolls over. Only used if Rollover Type is SIZE or BOTH.
Rollover Type	SIZE	Type of log rollover. Valid values are SIZE, TIME, NONE or BOTH. The default is SIZE.

Parameters for Configure WebSphere Cluster and Cluster Members

The following tables describe the required and optional input parameters for this workflow. Most of these parameters are not initially visible in a deployment. For most parameters, if you do not specify a value for a parameter, a default value is assigned.

Parameters Defined in this Step: Configure WebSphere Cluster Parameters

Parameter Name	Default Value	Required	Description
Cluster Member Name	no default	required	The base cluster member name that will be used for each cluster member/application server. A suffix will automatically be appended to this base name that will indicate the node and cluster. For the initial cluster, the suffixes will be 001a for the first node, 001b for second node, and so on. If a vertical cluster member is created, the suffixes will be 002a for the first node, 002b for the second node, and so on. It cannot contain any of the following characters / \ * , ; = + ? < > & % ' " [] # \$ ^ { }.
Cluster Name	no default	required	This is the name given to the logical grouping of cluster members. This name has to be unique to the cell. It cannot contain any of the following characters / \ * , ; = + ? < > & % ' " [] # \$ ^ { }.
Enable Security	no default	required	Indicates whether security will be enabled. Valid values are True or False. If True then WebSphere Admin Password and WebSphere Admin User must have values.
Number Cluster Members	no default	required	The number of cluster members/application servers that will be created on each node.
Web Service Password	no default	required	Password for the DMA Discovery web service API.
Web Service URL	no default	required	URL for the DMA Discovery web service API. For example: <code>https://example.com:8443/dma</code>
Web Service User	no default	required	A user capable of modifying the DMA managed environment by using the web service API.
WebSphere Admin Password	no default	optional	The password for a user in a group that can change the state of a given application server. Only required if global security is enabled. It cannot begin with a dash (-) or contain a space ().
WebSphere Admin Username	no default	optional	The user account for a user in a group that can change the state of a given application server. Only required if global security is enabled. It cannot begin with a dash (-), a period (.), or a space (). It cannot contain any of the following characters / \ * , ; = + ? < > & % ' " [] # \$ ^ { }.

Additional Parameters Defined in this Step: JVM Parameters for Configure WebSphere Cluster Members

Parameter Name	Default Value	Required	Description
Initial Heap Size	see description	optional	Initial heap size, in megabytes, that all cluster members will be set to on creation. The default is the WebSphere default value.
Maximum Heap Size	see description	optional	Maximum heap size, in megabytes, that all cluster members will be set to on creation. The default is the WebSphere default value.

Additional Parameters Defined in this Step: Logging Parameters for Configure WebSphere Cluster Members

Parameter Name	Default Value	Required	Description
Base Hour	no default	optional	The hour of the day, from 1 to 24, when the periodic rollover starts. The rollover always starts at the specified hour of the day. Hour 1 is 00:00:00 (midnight) and hour 24 is 23:00:00. Once started, the rollover repeats every Rollover Period hours.
Logfile Location	no default	optional	Fully qualified directory path where the SystemOut and SystemErr logs will be created. For example: /app/logs
Maximum Rollback Files	no default	optional	The number of historical logs to keep.
Rollover Period	no default	optional	The number of hours after which the log file rolls over. Valid values range from 1 to 24. Only used if Rollover Type is TIME or BOTH.
Rollover Size	no default	optional	The maximum size of the log file in megabytes. When the file reaches this size, it rolls over. Only used if Rollover Type is SIZE or BOTH.
Rollover Type	no default	optional	Type of log rollover. Valid values are SIZE, TIME, NONE or BOTH. The default is SIZE.

WebSphere - Configure IBM HTTP Server

The workflow picks an existing instance of IBM WebSphere Application Server, connects it to a specific DManager profile provided, and creates a WebServer definition in DManager profile. This workflow also generates the plugin configuration XML file for that profile and propagates the XML file to the IBM HTTP Server location.

This workflow creates IBM HTTP Server definition in a profile of IBM WebSphere Application Server 8.0 or 8.5.x on Linux 5, 6, and 7, SUSE 11, Windows 2008 R2, Solaris 10, and AIX.

Note: The propagation of XML file is not implemented in Windows Operating System.

To use this workflow in your environment, see the following information:

Topic	Information Included
"Prerequisites for this Workflow"	List of prerequisites that must be satisfied before you can run this workflow
"How this Workflow Works"	Information about what the workflow does, including validation checks performed, steps executed, and a high-level process flow
"How to run this workflow "	Instructions for running this workflow in your environment
"Parameters for WebSphere - Configure IBM HTTP Server" on page 1430	List of input parameters for this workflow

Note: The documentation for this workflow contains steps that are referred to by their base names. The names in the DMA user interface may have a version appended, for example, v2.

Prerequisites for this Workflow

Be sure that the following prerequisites are satisfied before you run this workflow:

1. You have installed the DMA ASConfigManagement solution pack.
2. You have a valid HP Software support contract for this solution pack.
3. You have downloaded and installed all available DMA patches and hot fixes.
4. IBM Installation Manager software exists on each target machine.

For specific target operating system versions supported by each workflow, see the *Database and Middleware Automation Support Matrix*.

Dependencies:

The WebSphere - Configure IBM HTTP Server workflow requires the following:

- Unrestricted sudo access to the user (typically root) who can access all the required files and directories.
- An instance of the IBM WebSphere Application Server installed on the target machine.
- An installation location of IBM HTTP Server on a machine.
- The credentials of the remote machine or the target machine on which the workflow will be run, for propagating the plugin configuration xml file.

For information about prerequisites for WebSphere 8.0 or 8.5.x, refer to the [IBM HTTP Server 8.5 Product Documentation](#).

How this Workflow Works

The following information describes how the ["WebSphere - Configure IBM HTTP Server" on page 1424](#) workflow works:

Overview

This workflow connects to a specific DManager profile provided by the user of an existing instance of IBM WebSphere Application Server creates a WebServer definition in DManager profile.

Steps Executed

The WebSphere - Configure IBM HTTP Server workflow includes the following steps. Each step must complete successfully before the next step can start. If a step fails, the workflow restores the configuration, cleans up files as necessary, reports a failure, and skips all subsequent steps.

Steps for IBM HTTP Server - Patch Software

Workflow Step	Description
Gather Parameters for Configure IBM HTTP Server	Gathers the required parameters needed to configure the IBM WebSphere Application Server V8.0 and 8.5.x for IBM HTTP Server.
Gather Advanced Parameters for Configure IBM HTTP Server	Gathers the optional parameters needed to configure the IBM WebSphere Application Server V8.0 and 8.5.x for IBM HTTP Server.
Get WSAdmin Call Wrapper	Creates the necessary call wrapper to call wsadmin to execute certain operations within a given WebSphere environment.
Validate Parameters for Configure IBM HTTP Server	Validates the basic and advanced parameters provided by the user, and checks the prerequisites for configuring the IBM WebSphere Application Server for IBM HTTP Server.
Create IBM HTTP Server Definition	Creates IBM HTTP Server definition in the IBM WebSphere Application Server.
Generate Plugin Configuration XML	Generates the Plugin configuration XML files of the IBM HTTP Server definition created in the IBM WebSphere Application Server.
WebSphere - Propagate Plugin Config XML	Transfers the generated Plugin configuration XML files of the IBM HTTP Server definition created in the IBM WebSphere Application Server.
Discover WebSphere	<p>Audits the server's physical environment looking for IBM HTTP Server instances.</p> <p>Note: Discovery is ONLY additive. It will not remove instances or databases currently in your environment. It is your DMA administrator's responsibility to delete content that is no longer in use.</p>

For parameter descriptions and defaults, see ["Parameters for WebSphere - Configure IBM HTTP Server" on page 1430](#).

How to run this workflow

The following instructions show you how to customize and run the ["WebSphere - Configure IBM HTTP Server" on page 1424](#) workflow in your environment.

Note: Before following this procedure, review the ["Prerequisites for this Workflow" on page 1425](#), and ensure that all requirements are satisfied.

To use the WebSphere - Configure IBM HTTP Server workflow:

1. Create a deployable copy of the workflow.
2. Determine the values that you will specify for the following parameters: show

Parameter Name	Default Value	Required	Description
Enable Security	no default	required	The values of this parameter can be True or False. If the value of this parameter is True, the values of the WAS Admin Password and WAS Admin User parameters must also be specified.
Profile Name	no default	required	The profile name for configuring the IBM HTTP Server.
WAS Admin Password	no default	required	If the value of the Enable Security parameter is True, the value of this parameter must be specified. If not, keep the field empty.
WAS Admin User	no default	required	If the value of the Enable Security parameter is True, the value of this parameter must be specified. If not, keep the field empty.
WebServer Admin Password	no default	required	IBM HTTP Server Admin password for administering from the WebSphere Application Server.
WebServer Admin Port	no default	required	IBM HTTP Server Admin port number for administering from WebSphere Application Server.
WebServer Admin User ID	no default	required	IBM HTTP Server Admin user ID for administering from WebSphere Application Server.
WebServer Configuration File	no default	required	IBM HTTP Server configuration file for administering from WebSphere Application Server.
WebServer Hostname	no default	required	Host name of the machine where IBM HTTP server is installed.
WebServer Install Location	no default	required	Fully qualified path of the IBM HTTP Server installation directory.

, continued

Parameter Name	Default Value	Required	Description
WebServer Name	no default	required	Name for creating the IBM HTTP Server entry in the WebSphere Application Server.
WebServer Node Name	no default	required	The node name under which the IBM HTTP Server is federated.
WebServer Plugin Install Location	no default	required	Fully qualified path of the WebServer Plugin install location.
WebServer Port	no default	required	The port number of the IBM HTTP Server instance runs.
WebSphere Install Location	no default	required	Fully qualified path of the specific IBM WebSphere Application Server installation where the profile root is present.

Tip: To avoid having to re-enter passwords whenever they change, you can create a policy to provide them to the workflow.

Note: See ["Parameters for WebSphere - Configure IBM HTTP Server" on the next page](#) for detailed descriptions of all input parameters for this workflow, including default values.

3. In the workflow editor, expose any additional parameters that you need. You will specify values for those parameters when you create the deployment.
4. Save the changes to the workflow (click **Save** in the lower right corner).
5. Create a new deployment.
6. On the Parameters tab, specify values for the required parameters listed in step 2 and any additional parameters that you have exposed. You do not need to specify values for those parameters whose default values are appropriate for your environment.
7. On the Targets tab, specify one or more targets for this deployment.
8. Save the deployment (click **Save** in the lower right corner).
9. Run the workflow using this deployment.

To verify the results:

The workflow will complete and report SUCCESS on the Console if it has run successfully. If an error occurs during workflow execution, the error is logged, and the workflow terminates in the FAILURE state.

Parameters for WebSphere - Configure IBM HTTP Server

The following tables describe the required and optional input parameters for this workflow. Most of these parameters are not initially visible in a deployment. For many parameters, if you do not specify a value for a parameter, a default value is assigned

Input Parameters Defined in this Step: Gather Parameters for Configure IBM HTTP Server

Parameter Name	Default Value	Required	Description
Enable Security	no default	required	The values of this parameter can be True or False. If the value of this parameter is True, the values of the WAS Admin Password and WAS Admin User parameters must also be specified.
Profile Name	no default	required	The profile name for configuring the IBM HTTP Server.
WAS Admin Password	no default	required	If the value of the Enable Security parameter is True, the value of this parameter must be specified. If not, keep the field empty.
WAS Admin User	no default	required	If the value of the Enable Security parameter is True, the value of this parameter must be specified. If not, keep the field empty.
WebServer Admin Password	no default	required	IBM HTTP Server Admin password for administering from the WebSphere Application Server.
WebServer Admin Port	no default	required	IBM HTTP Server Admin port number for administering from WebSphere Application Server.
WebServer Admin User ID	no default	required	IBM HTTP Server Admin user ID for administering from WebSphere Application Server.
WebServer Configuration File	no default	required	IBM HTTP Server configuration file for administering from WebSphere Application Server.
WebServer Hostname	no default	required	Host name of the machine where IBM HTTP server is installed.
WebServer Install Location	no default	required	Fully qualified path of the IBM HTTP Server installation directory.
WebServer Name	no default	required	Name for creating the IBM HTTP Server entry in the WebSphere Application Server.
WebServer Node Name	no default	required	The node name under which the IBM HTTP Server is federated.
WebServer Plugin Install Location	no default	required	Fully qualified path of the WebServer Plugin install location.
WebServer	no	required	The port number of the IBM HTTP Server instance runs.

Input Parameters Defined in this Step: Gather Parameters for Configure IBM HTTP Server, continued

Parameter Name	Default Value	Required	Description
Port	default		
WebSphere Install Location	no default	required	Fully qualified path of the specific IBM WebSphere Application Server installation where the profile root is present.

Additional Input Parameters Defined in this Step: Gather Advanced Parameters for Provision IBM HTTP Server

Parameter Name	Default Value	Required	Description
Call Wrapper	no default	required	Command that executes the step as a specific user. By default, sudo su - root /opt/hp/dma/client/bin/jython.sh on UNIX targets and jython running as Administrator on Windows targets.
Cleanup on Success	True	optional	Indicates whether to remove downloaded and extracted files and to clean up the installation directory in the event of workflow success. Valid values are True and False. The default is True, which will clean up on success.
Destination Directory	no default	optional	Destination directory of the remote host where the plugin configuration xml files will be transferred.
Map Applications	no default	optional	Determines if all the applications installed on the application server will be mapped to the plugin configuration xml.
Propagate XML	False	optional	Determines whether to transfer the Plugin configuration XML files to the remote host.
Remote Host Password	no default	optional	Password to transfer the plugin configuration XML files to the remote host.
Remote Host Username	no default	optional	Username to transfer the plugin configuration XML files to the remote host.
WebServer Node Type	no default	optional	The type of the WebServer Node for IBM HTTP Server can be managed or unmanaged

Sample Scenario

This topic shows you typical parameter values used for the ["WebSphere - Configure IBM HTTP Server"](#) workflow.

Tip: To avoid having to re-enter passwords whenever they change, you can create a policy to provide them to the workflow.

Scenario 1:

Configure IBM HTTP Server with root - Parameter Value Examples

Parameter Name	Example Value	Description
Enable Security		The values of this parameter can be True or False. If the value of this parameter is True, the values of the WAS Admin Password and WAS Admin User parameters must also be specified.
Profile Name		The profile name for configuring the IBM HTTP Server.
WAS Admin Password		If the value of the Enable Security parameter is True, the value of this parameter must be specified. If not, keep the field empty.
WAS Admin User		If the value of the Enable Security parameter is True, the value of this parameter must be specified. If not, keep the field empty.
WebServer Admin Password		IBM HTTP Server Admin password for administering from the WebSphere Application Server.
WebServer Admin Port		IBM HTTP Server Admin port number for administering from WebSphere Application Server.
WebServer Admin User ID		IBM HTTP Server Admin user ID for administering from WebSphere Application Server.
WebServer Configuration File		IBM HTTP Server configuration file for administering from WebSphere Application Server.
WebServer Hostname		Host name of the machine where IBM HTTP server is installed.
WebServer Install Location		Fully qualified path of the IBM HTTP Server installation directory.
WebServer Name		Name for creating the IBM HTTP Server entry in the WebSphere Application Server.
WebServer Node Name		The node name under which the IBM HTTP Server is federated.
WebServer		Fully qualified path of the WebServer Plugin install

Configure IBM HTTP Server with root - Parameter Value Examples, continued

Parameter Name	Example Value	Description
Plugin Install Location		location.

Scenario 2:**Configure IBM HTTP Server with non-root - Parameter Value Examples**

Parameter Name	Example Value	Description
Enable Security		The values of this parameter can be True or False. If the value of this parameter is True, the values of the WAS Admin Password and WAS Admin User parameters must also be specified.
Profile Name		The profile name for configuring the IBM HTTP Server.
WAS Admin Password		If the value of the Enable Security parameter is True, the value of this parameter must be specified. If not, keep the field empty.
WAS Admin User		If the value of the Enable Security parameter is True, the value of this parameter must be specified. If not, keep the field empty.
WebServer Admin Password		IBM HTTP Server Admin password for administering from the WebSphere Application Server.
WebServer Admin Port		IBM HTTP Server Admin port number for administering from WebSphere Application Server.
WebServer Admin User ID		IBM HTTP Server Admin user ID for administering from WebSphere Application Server.
WebServer Configuration File		IBM HTTP Server configuration file for administering from WebSphere Application Server.
WebServer Hostname		Host name of the machine where IBM HTTP server is installed.
WebServer Install Location		Fully qualified path of the IBM HTTP Server installation directory.
WebServer Name		Name for creating the IBM HTTP Server entry in the WebSphere Application Server.
WebServer Node Name		The node name under which the IBM HTTP Server is federated.
WebServer Plugin Install Location		Fully qualified path of the WebServer Plugin install location.
WebServer Port		The port number of the IBM HTTP Server instance runs.

Configure IBM HTTP Server with non-root - Parameter Value Examples, continued

Parameter Name	Example Value	Description
WebSphere Install Location		Fully qualified path of the specific IBM WebSphere Application Server installation where the profile root is present.

Scenario 3:**Configure IBM HTTP Server, plug-in, and HTTP Admin Server with non-root - Parameter Value Examples**

Parameter Name	Example Value	Description
Enable Security		The values of this parameter can be True or False. If the value of this parameter is True, the values of the WAS Admin Password and WAS Admin User parameters must also be specified.
Profile Name		The profile name for configuring the IBM HTTP Server.
WAS Admin Password		If the value of the Enable Security parameter is True, the value of this parameter must be specified. If not, keep the field empty.
WAS Admin User		If the value of the Enable Security parameter is True, the value of this parameter must be specified. If not, keep the field empty.
WebServer Admin Password		IBM HTTP Server Admin password for administering from the WebSphere Application Server.
WebServer Admin Port		IBM HTTP Server Admin port number for administering from WebSphere Application Server.
WebServer Admin User ID		IBM HTTP Server Admin user ID for administering from WebSphere Application Server.
WebServer Configuration File		IBM HTTP Server configuration file for administering from WebSphere Application Server.
WebServer Hostname		Host name of the machine where IBM HTTP server is installed.
WebServer Install Location		Fully qualified path of the IBM HTTP Server installation directory.
WebServer Name		Name for creating the IBM HTTP Server entry in the WebSphere Application Server.
WebServer Node Name		The node name under which the IBM HTTP Server is federated.
WebServer Plugin Install Location		Fully qualified path of the WebServer Plugin install location.

Configure IBM HTTP Server, plug-in, and HTTP Admin Server with non-root - Parameter Value Examples, continued

Parameter Name	Example Value	Description
WebServer Port		The port number of the IBM HTTP Server instance runs.
WebSphere Install Location		Fully qualified path of the specific IBM WebSphere Application Server installation where the profile root is present.

Scenario 4:

Configure IBM HTTP Server, plug-in, HTTP Admin Server, and HTTP SSL with non-root - Parameter Value Examples

Parameter Name	Example Value	Description
Enable Security		The values of this parameter can be True or False. If the value of this parameter is True, the values of the WAS Admin Password and WAS Admin User parameters must also be specified.
Profile Name		The profile name for configuring the IBM HTTP Server.
WAS Admin Password		If the value of the Enable Security parameter is True, the value of this parameter must be specified. If not, keep the field empty.
WAS Admin User		If the value of the Enable Security parameter is True, the value of this parameter must be specified. If not, keep the field empty.
WebServer Admin Password		IBM HTTP Server Admin password for administering from the WebSphere Application Server.
WebServer Admin Port		IBM HTTP Server Admin port number for administering from WebSphere Application Server.
WebServer Admin User ID		IBM HTTP Server Admin user ID for administering from WebSphere Application Server.
WebServer Configuration File		IBM HTTP Server configuration file for administering from WebSphere Application Server.
WebServer Hostname		Host name of the machine where IBM HTTP server is installed.
WebServer Install Location		Fully qualified path of the IBM HTTP Server installation directory.
WebServer Name		Name for creating the IBM HTTP Server entry in the WebSphere Application Server.
WebServer Node Name		The node name under which the IBM HTTP Server is federated.
WebServer		Fully qualified path of the WebServer Plugin install location.

Configure IBM HTTP Server, plug-in, HTTP Admin Server, and HTTP SSL with non-root - Parameter Value Examples, continued

Parameter Name	Example Value	Description
Plugin Install Location		
WebServer Port		The port number of the IBM HTTP Server instance runs.
WebSphere Install Location		Fully qualified path of the specific IBM WebSphere Application Server installation where the profile root is present.

IBM HTTP Server - RollBack Patch Software

This workflow picks an existing instance of IBM HTTP Server and rolls back to a specific Patch ID of the IBM HTTP Server. This workflow takes into account the multiple instances related to a specific installation of the aforementioned IBM HTTP server and ensures all its components (server instances) are stopped before patching.

This workflow rollback to a specific patch ID of IBM HTTP Server 8.0 or 8.5.x using an existing Install Manager on Linux 5, 6, and 7, SUSE 11, Windows 2008 R2, Solaris 10, and AIX.

To use this workflow in your environment, see the following information:

Topic	Information Included
"Prerequisites for this workflow" on the next page	List of prerequisites that must be satisfied before you can run this workflow
"How this workflow works" on page 1438	Information about what the workflow does, including validation checks performed, steps executed, and a high-level process flow
"How to run this workflow " on page 1442	Instructions for running this workflow in your environment
"Parameters for IBM HTTP Server - Rollback Patch Software" on page 1444	List of input parameters for this workflow

Prerequisites for this workflow

Be sure that the following prerequisites are satisfied before you run this workflow:

1. You have installed the DMA AS Patching solution pack.
2. You have a valid HP Software support contract for this solution pack.
3. You have downloaded and installed all available DMA patches and hot fixes.
4. IBM Installation Manager software exists on each target machine.

For specific target operating system versions supported by each workflow, see the *Database and Middleware Automation Support Matrix*.

Dependencies:

- The workflow requires unrestricted sudo access to the user, typically root user, who can access all the required files and directories.
- The workflow requires that an instance of IBM Installation Manager be installed on each of the target servers.
- The workflow supports the patching of IHS 8.0 or 8.5.x running on a machine.

For information about prerequisites for WebSphere 8.0 or 8.5.x, refer to the [IBM HTTP Server 8.5 Product Documentation](#).

How this workflow works

The following information describes how the ["IBM HTTP Server - RollBack Patch Software" on page 1436](#) workflow works:

Overview

This workflow picks an existing instance of IBM HTTP Server and rolls back to a specific Patch ID of the IBM HTTP Server. This workflow takes into account the multiple instances related to a specific installation of the aforementioned IBM HTTP server and ensures all its components (server instances) are stopped before patching.

Steps Executed

The IBM HTTP Server - RollBack Patch Software workflow includes the following steps. Each step must complete successfully before the next step can start. If a step fails, the workflow restores the configuration, cleans up files as necessary, reports a failure, and skips all subsequent steps.

Steps for IBM HTTP Server - RollBack Patch Software

Workflow Step	Description
Gather Parameters for IBM HTTP Server - RollBack Patch Software	Gathers the required parameters needed to patch the IBM HTTP Server V8.0 and 8.5.x.
Gather Advanced Parameters for IBM HTTP Server - RollBack Patch Software	Gathers the optional parameters needed to patch the IBM HTTP Server V8.0 and 8.5.x.
Validate Parameters for IBM HTTP Server - RollBack Patch Software	This step validates the basic and advanced parameters provided by the user, and checks the prerequisites for patching the IBM HTTP Server.
Check File Download	Check for the existence of a file before downloading from Expert Engine. Check if file is in the expected place. If file is not in the expected location, output data for file download.
Download Software	Automates the transfer of files from the software repository to individual managed servers for use in downstream workflow steps.
Verify Install Manager Exists	Verifies that an IBM Installation Manager instance exists on each of the specified target machines.
WebSphere 8 Patching Extract Archive v2	First checks to ensure that the archive file exists. Then, based on the archive extension, extracts the archive to the specified directory.
IBM HTTP Server Stop Application Servers	This step takes a list of IBM - HTTP Servers, checks the state of each application server, and stops only the application servers that are in a started state.
Verify All IHS Processes Stopped	This step validates that all server instances on a given machine have been stopped.
IBM HTTP Server RollBack Patch	This step utilizes the WebSphere Install Manager to apply the cumulative patches to a given HTTPServer installation.
IBM HTTP Server Start Application Servers	This step takes a list of HTTP Servers, checks the state of each application server, and starts only the application servers that were stopped by the IBM - HTTPServer Stop Application Server step.
IBM HTTP Server Start Application Servers	This step takes a list of HTTP Servers, checks the state of each application server, and starts only the application servers that were stopped by the IBM - HTTPServer Stop Application Server step.
Discover IBM HTTP Server	This step audits the server's physical environment looking for IBM HTTP Server instances.

Steps for IBM HTTP Server - RollBack Patch Software, continued

Workflow Step	Description
	Note: Discovery is only additive. It will not remove instances or databases currently in your environment. It is your DMA administrator's responsibility to delete content that is no longer in use.
Cleanup Downloaded Files	Removes all downloaded files and archives.

For parameter descriptions and defaults, see ["Parameters for IBM HTTP Server - Rollback Patch Software" on page 1444](#).

How to run this workflow

The following instructions show you how to customize and run the ["IBM HTTP Server - RollBack Patch Software" on page 1436](#) workflow in your environment.

Note: Before following this procedure, review the ["Prerequisites for this workflow" on page 1437](#), and ensure that all requirements are satisfied.

To use the IBM HTTP Server - Rollback Patch Software workflow:

1. Create a deployable copy of the workflow.
2. Determine the values that you will specify for the following parameters:

Parameter Name	Default Value	Required	Description
IHS Install Location	no default	required	Fully qualified directory path of the specific IBM HTTP Server installation which needs to be patched.
IHS Patch File List	no default	required	Comma separated list of patch files to be patched. For example: 8.0.0-WS-WASSupplements-FP0000003-part1.zip, 8.0.0-WS-WASSupplements-FP0000003-part2.zip
IHS Patch ID	no default	required	Patch ID of the IBM HTTP Server to be rollbacked to. For example: com.ibm.websphere.IHS.v85_8.5.5000.20130514_1044
Staging Location	no default	required	The list of patch files that are downloaded.

Tip: To avoid having to re-enter passwords whenever they change, you can create a policy to provide them to the workflow.

Note: See ["Parameters for IBM HTTP Server - Rollback Patch Software" on page 1444](#) for detailed descriptions of all input parameters for this workflow, including default values.

3. In the workflow editor, expose any additional parameters that you need. You will specify values for those parameters when you create the deployment.
4. Save the changes to the workflow (click **Save** in the lower right corner).
5. Create a new deployment.
6. On the Parameters tab, specify values for the required parameters listed in step 2 and any additional parameters that you have exposed. You do not need to specify values for those parameters whose default values are appropriate for your environment.

7. On the Targets tab, specify one or more targets for this deployment.
8. Save the deployment (click **Save** in the lower right corner).
9. Run the workflow using this deployment.

To verify the results:

The workflow will complete and report SUCCESS on the Console if it has run successfully. If an error occurs during workflow execution, the error is logged, and the workflow terminates in the FAILURE state.

Parameters for IBM HTTP Server - Rollback Patch Software

The following tables describe the required and optional input parameters for this workflow.

Parameters Defined in this Step: Gather Parameters For IBM HTTP Server - Rollback Patch Software

Parameter Name	Default Value	Required	Description
IHS Install Location	no default	required	Fully qualified directory path of the specific IBM HTTP Server installation which needs to be patched.
IHS Patch File List	no default	required	Comma separated list of patch files to be patched. For example: 8.0.0-WS-WASSupplements-FP0000003-part1.zip, 8.0.0-WS-WASSupplements-FP0000003-part2.zip
IHS Patch ID	no default	required	Patch ID of the IBM HTTP Server to be rolled back to. For example: com.ibm.websphere.IHS.v85_8.5.5000.20130514_1044
Staging Location	no default	required	The list of patch files that are downloaded.

Parameters Defined in this Step: Gather Advanced Parameters For IBM HTTP Server - Rollback Patch Software

Parameter Name	Default Value	Required	Description
Cleanup on Failure	True	optional	Determines whether or not to remove downloaded and extracted files. This parameter also cleans up the installed directory upon failure of the workflow.
Cleanup on Success	True	optional	Determines whether or not to remove downloaded and extracted files. This parameter also cleans up the installed directory upon successful execution of the workflow.
WebServer Plugin Location	True	optional	WebServer Plugin Location to be patched
WebServer Plugin Patch ID	no default	optional	WebServer Plugin Patch ID to which the installation will be rolled back to

WebSphere 8 - Rollback Patch Network Cell

This workflow picks an existing instance of IBM Install Manager and rolls back to a particular patch level of a specific installation of the IBM WebSphere Application Server.

This workflow takes into account the multiple components related to a Network Deployment implementation and makes sure that all components (dmgr, nodeagent, and application servers) are stopped before rolling back the patch.

To use this workflow in your environment, see the following information:

Topic	Information Included
"Prerequisites for this Workflow"	List of prerequisites that must be satisfied before you can run this workflow
"How this Workflow Works"	Information about what the workflow does, including validation checks performed, steps executed, and a high-level process flow
"How to Run this Workflow "	Instructions for running this workflow in your environment
"Parameters for WebSphere 8 - Patch Network Cell" on page 1453	List of input parameters for this workflow

Prerequisites for this Workflow

Be sure that the following prerequisites are satisfied before you run this workflow:

1. You have installed the DMA Application Server Patching solution pack.
2. You have a valid HP Software support contract for this solution pack.
3. You have downloaded and installed all available DMA patches and hot fixes.
4. IBM Installation Manager software exists on each target machine.

For specific target operating system versions supported by each workflow, see the *Database and Middleware Automation Support Matrix* available on the Software Support web site:

<https://softwaresupport.hp.com/>

Dependencies:

- The workflow requires unrestricted sudo access to the user, typically root user, who can access all the required files and directories.
- The workflow requires that an instance of IBM Installation Manager be installed on each of the target servers.
- The workflow supports the patching of IHS 8.0 or 8.5.x running on a machine.

For information about prerequisites for WebSphere 8.0 or 8.5.x, refer to the [WebSphere 8 Product Documentation](#).

How this Workflow Works

The following information describes how the ["WebSphere 8 - Rollback Patch Network Cell" on page 1445](#) workflow works:

Overview

This workflow picks an existing instance of IBM Install Manager and rolls back to a particular patch level of a specific installation of the IBM WebSphere Application Server.

Validation Checks Performed

The validation centers on the input parameters:

- The input parameters have the proper syntax (no special characters or spaces).
- Specified files exist and have valid permissions.

Steps Executed

The WebSphere 8 - Rollback Patch Network Cell workflow includes the following steps. Each step must complete successfully before the next step can start. If a step fails, the workflow restores the configuration, cleans up files as necessary, reports a failure, and skips all subsequent steps.

Steps for WebSphere 8 - Rollback Patch Network Cell

Workflow Step	Description
Gather Parameters For WebSphere 8 Network Cell Rollback Patch	Gathers the required parameters needed to patch the IBM WebSphere Application Server V8.0 and 8.5.x.
Gather Advanced Parameters For WebSphere 8 Network Cell Rollback Patch	Gathers the optional parameters needed to patch the IBM WebSphere Application Server V8.0 and 8.5.x.
Get WSAAdmin Call Wrapper	Creates the necessary call wrapper to call <code>wsadmin</code> to execute certain operations within the WebSphere 8.0 or 8.5.x environment.
Validate Parameters For WebSphere 8 Rollback Patch Network Cell	This step validates the basic and advanced parameters provided by the user, and checks the prerequisites for patching the IBM WebSphere Application Server.
Check File Download	Checks for the existence of a file on the target machine before downloading that file from the DMA server. For each file in the list: <ol style="list-style-type: none"> 1. The step determines whether the file is in the expected location on the target machine. 2. If the file is not in the expected location, the step adds that file to a list of files that need to be downloaded.
Download Software	Automates the transfer of files from the software repository to individual managed servers for use in downstream workflow steps.
WebSphere8 Backup Config	Uses the <code>backupConfig</code> utility to backup the WebSphere configurations for the specified WebSphere 8.0 or 8.5.x installation.
Verify Install Manager Exists	Verifies that an IBM Installation Manager instance exists on each of the specified target machines.
WebSphere 8 Patching Extract Archive v2	First checks to ensure that the archive file exists. Then, based on the archive extension, extracts the archive to the specified directory.
WebSphere Stop Application Servers v2	Stops all application servers that are in started state before patching the installation of WebSphere.
WebSphere 8 Stop Management Processes v2	First stops <code>nodeagents</code> . If there is a <code>dmgr</code> process running, the step will then stop that process before patching the WebSphere 8.0 or 8.5.x installation.
Verify All Java Processes Stopped	Verifies that all Java processes relevant to the WebSphere services on the specified target have been stopped.
WebSphere 8 Rollback Patch	Uses the IBM Installation Manager to rollback

Steps for WebSphere 8 - Rollback Patch Network Cell, continued

Workflow Step	Description
	patch to the given WebSphere installation.
WebSphere 8 Start Management Processes v2	First starts the <code>dmgr</code> process first if one exists. Then, starts the <code>nodeagent</code> process.
WebSphere 8 Restore Config	If the patching process fails, this step is called to restore the configuration via the <code>restoreConfig</code> utility.
WebSphere Start Application Servers v2	Starts only the application servers that were stopped by the WebSphere Stop Application Servers step.
WebSphere 8 Start Management Processes v2	First starts the <code>dmgr</code> process first if one exists. Then, starts the <code>nodeagent</code> process.
Cleanup Downloaded Files v2	Removes all temporary downloaded files and archives.
WebSphere Start Application Servers v2	Starts only the application servers that were stopped by the WebSphere Stop Application Servers step.
Discover WebSphere	<p>This step audits the server's physical environment looking for WebSphere cells, clusters, and managed servers..</p> <p>Note: Discovery is only additive. It will not remove instances or databases currently in your environment. It is your DMA administrator's responsibility to delete content that is no longer in use.</p>

For parameter descriptions and defaults, see [Parameters for WebSphere 8 - Patch Network Cell](#).

How to Run this Workflow

The following instructions show you how to customize and run the "WebSphere 8 - Rollback Patch Network Cell" workflow in your environment.

Note: Before following this procedure, review the "Prerequisites for this Workflow" on page 1446, and ensure that all requirements are satisfied.

To use the WebSphere 8 - Rollback Patch Network Cell workflow:

1. Create a deployable copy of the workflow.
2. Determine the values that you will specify for the following parameters:

Parameter Name	Default Value	Required	Description
Config Backup File	no default	required	Fully qualified file path where the WebSphere BackupConfig utility will write the backup file. For example: /opt/IBM/WebSphere/newbackup/backup.zip
Enable Security	no default	required	Enables administrative security. Must be set to either true or false. If Enable Security is true, the WAS Admin User and WAS Admin Password parameters must have values.
WAS Admin Password	no default	required	If security is enabled, this is the password for a user who belongs to a group that has permission to change the state of a specific application server.
WAS Admin User	myUsername	required	If security is enabled, this is the user account for a user who belongs to a group that has permission to change the state of a specific application server.
WebSphere Install Location	see description	required	Fully qualified file path of the specific IBM WebSphere Application Server installation which needs to be patched. For example: /usr/IBM/WebSphere/AppServer or /opt/IBM/WebSphere/AppServer
WebSphere Patch File List	no default	required	Comma-separated list of WebSphere cumulative patch files on the target machine. For example: 8.0.0-WS-WAS-FP0000003-part1.zip, 8.0.0-WS-WAS-FP0000003-part2.zip
WebSphere Patch ID	no default	required	WebSphere Patch ID to which Installation will be rolled back to.
WebSphere Staging Location	no default	required	Fully qualified file path of the location where the list of patch files are downloaded.

Tip: To avoid having to re-enter passwords whenever they change, you can create a policy to provide them to the workflow.

Note: See "[Parameters for WebSphere 8 - Patch Network Cell](#)" on the next page for detailed descriptions of all input parameters for this workflow, including default values.

3. In the workflow editor, expose any additional parameters that you need. You will specify values for those parameters when you create the deployment.
4. Save the changes to the workflow (click **Save** in the lower right corner).
5. Create a new deployment.
6. On the Parameters tab, specify values for the required parameters listed in step 2 and any additional parameters that you have exposed. You do not need to specify values for those parameters whose default values are appropriate for your environment.
7. On the Targets tab, specify one or more targets for this deployment.
8. Save the deployment (click **Save** in the lower right corner).
9. Run the workflow using this deployment.

To verify the results:

The workflow will complete and report SUCCESS on the Console if it has run successfully. If an error occurs during workflow execution, the error is logged, and the workflow terminates in the FAILURE state.

Parameters for WebSphere 8 - Patch Network Cell

The following tables describe the required and optional input parameters for this workflow.

Parameters Defined in this Step: Gather Parameters For WebSphere 8 Network Cell Patching

Parameter Name	Default Value	Required	Description
Config Backup File	no default	required	Fully qualified file path where the WebSphere BackupConfig utility will write the backup file. For example: /opt/IBM/WebSphere/newbackup/backup.zip
Enable Security	true	required	Enables administrative security. Must be set to either true or false. If Enable Security is true, the WAS Admin User and WAS Admin Password parameters must have values.
WAS Admin Password	myPwd	required	If global security is enabled, this is the password for a user who belongs to a group that has permission to change the state of a specific application server.
WAS Admin User	myUsername	required	If global security is enabled, this is the user account for a user who belongs to a group that has permission to change the state of a specific application server.
WebSphere Install Location	see description	required	Fully qualified file path of the specific IBM WebSphere Application Server installation which needs to be patched. For example: /usr/IBM/WebSphere/AppServer or /opt/IBM/WebSphere/AppServer
WebSphere Patch File List	no default	required	Comma-separated list of WebSphere cumulative patch files on the target machine. For example: 8.0.0-WS-WAS-FP0000003-part1.zip, 8.0.0-WS-WAS-FP0000003-part2.zip
WebSphere Staging Location	no default	required	Fully qualified file path of the location where the list of patch files are downloaded. usr/IBM/patches/ or tmp/IBM/patches/

Parameters Defined in this Step: Gather Advanced Parameters For WebSphere 8 Network Cell Patching

Parameter Name	Default Value	Required	Description
Cleanup on Failure	True	Optional	Determines whether or not to remove downloaded and extracted files. This parameter also cleans up the installed directory upon failure of the workflow.
Cleanup on Success	True	Optional	Determines whether or not to remove downloaded and extracted files. This parameter also cleans up the installed directory upon successful execution of the workflow.

Promote Solution

This section includes the following topics:

Workflow type	Workflow name
Promoting	"Promote Workflow – Export" on the next page
	"Promote Workflow – Import" on page 1465
	"Promote Workflow – Export and Import" on page 1483

Promote Workflow – Export

To use this workflow in your environment, see the following information:

Topic	Information Included
"Prerequisites for this Workflow"	List of prerequisites that must be satisfied before you can run this workflow
"How This Workflow Works"	Information about what the workflow does, including validation checks performed, and steps executed
"How to Run This Workflow"	Instructions for running this workflow in your environment
"Sample Scenario"	Examples of typical parameter values for this workflow
Parameters	List of input parameters for this workflow

The information presented here assumes the following:

- DMA is installed and operational.
- At least one suitable target server is available.
- You are logged in to DMA as a user with Workflow Creator (or Administrator) capability.
- You have Read and Execute permission for the organization that contains your target server.

Prerequisites for this Workflow

Be sure that the following prerequisites are satisfied before you run the ["Promote Workflow – Export"](#) workflow:

- You are using Database and Middleware Automation version 10.50 (or later).
- You have installed the latest version of the Promote Solution Pack.
- Any roles required to modify or execute the workflow (or workflows) that will be promoted must exist on the destination DMA server.
- The DMA user who runs the workflow should have READ permission on the promoted items.

How This Workflow Works

"Promote Workflow – Export" exports the specified workflow and related components from the DMA server where you run the workflow (the source). It stores this information in a collection of XML files.

After you export a workflow, you can use "Promote Workflow – Import" to transfer this workflow (and specified related automation items) to a different DMA server (the destination).

By using these two workflows together, you can promote a customized workflow and all its components from one DMA server (the source) to another DMA server (the destination) in a reliable and replicable manner. This is useful, for example, when you want to move a workflow from a test environment to a production environment.



Process Flow

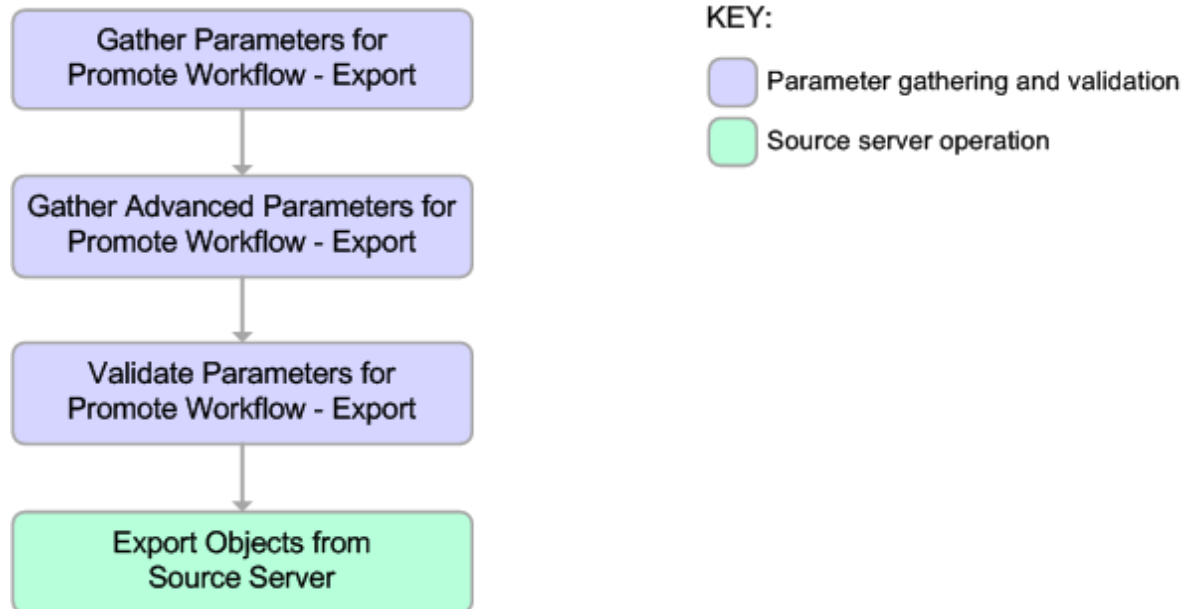
The workflow exports the workflow and the related automation items from the DMA source server, and stores this information in a collection of XML files in the Export Location.

The export process creates the `promote_info.txt` file.

1. The workflow, itself
2. Steps used in the workflow
3. Functions referenced by steps used in the workflow
4. Deployments associated with the workflow
5. Policies associated with any promoted deployment
6. Smart Groups associated with any promoted deployment
7. Custom Fields that are referenced by the workflow, any promoted deployment, any promoted step, or any promoted Smart Group

Steps Executed

Promote Workflow – Export includes the following steps. Each step must complete successfully before the next step can start. If a step fails, the workflow reports a failure and all subsequent steps are skipped.



Steps Used in Promote Workflow – Export

Workflow Step	Description
Gather Parameters for Promote Workflow – Export	Gets the name of the workflow to be promoted and Export Location. Sets the working directory/ZIP file.
Gather Advanced Parameters for Promote Workflow – Export	Gets the advanced optional parameter for this workflow: Export Zip Archive setting that specifies whether to export the workflow and related automation items as a ZIP archive or a sub-directory.
Validate Parameters for Promote Workflow – Export	<p>Verifies the following things:</p> <ul style="list-style-type: none"> • All required parameters have been specified. • The specified workflow exists on the source server, and the user has Read permission for that workflow.
Export Objects from Source Server	<p>Exports the workflow and the related automation items from the DMA source server, and stores this information in a collection of XML files in the working directory/ZIP file. Exports in the following order:</p> <ol style="list-style-type: none"> 1. The workflow, itself 2. Steps used in the workflow 3. Functions referenced by steps used in the workflow 4. Deployments associated with the workflow 5. Policies associated with any promoted deployment 6. Smart Groups associated with any promoted deployment 7. Custom Fields that are referenced by the workflow, any promoted deployment, any promoted step, or any promoted Smart Group <p>Creates the promote_info.txt file.</p>

Note: For input parameter descriptions and defaults, see "[Parameters for Promote Workflow – Export](#)" on page 1464.

How to Run This Workflow

The following instructions show you how to customize and run ["Promote Workflow – Export"](#) in your environment.

Note: Before following this procedure, review the ["Prerequisites for this Workflow"](#) on page 1456, and ensure that all requirements are satisfied.

Tip: As a best practice, set the target for the deployment to the DMA server where you run ["Promote Workflow – Export"](#).

To use the Promote Workflow – Export workflow:

1. On the DMA server where you run the workflow, create a deployable copy of the workflow.
2. Determine the values that you will specify for the following parameters:

Input Parameters for Gather Parameters for Promote Workflow - Export

Parameter Name	Default Value	Required	Description
Export Location	no default	required	The location where the exported DMA artifacts are stored. This can be either a fully qualified ZIP filename (default) or a fully qualified directory path—based on the advanced parameter Export Zip Archive. If it is a directory, a time-stamped sub-directory or ZIP file will be created to store the files. The location is on the target server.
Workflow Name	no default	required	Name of the workflow to be promoted.

3. Create a new deployment.
4. On the Parameters tab, specify values for the required parameters listed in step 2. You do not need to specify values for those parameters whose default values are appropriate for your environment.
5. On the Targets tab, specify a target for this deployment—where the exported workflow (and all related items) and the log files will be stored.

Tip: As a best practice, set the target to the DMA source server where the workflow is exported from.

6. Save the deployment (click **Save** in the lower right corner).
7. Run the workflow using this deployment.

To verify the results:

The workflow will complete and report SUCCESS on the Console if it has run successfully. If an error occurs during workflow execution, the error is logged, and the workflow terminates in the FAILURE state.

Results of each step are logged on the Output tab for each step. You can access this information from the Console page while the workflow is running or the History page after it finishes running.

You can examine the `promote_info.txt` file to determine specific information about the export.

To use the exported workflow:

The collection of exported XML files enables you to create a gold master of your workflow, its deployments, custom fields, policies, and permissions. This can be used in conjunction with a revision control system to help manage your production workflows.

You can use the exported workflow in the following ways:

- You can copy the exported working directory/ZIP file to an Archive.
- You can copy the exported working directory/ZIP file to the target server and working directory/ZIP file that you will use when you run "[Promote Workflow – Import](#)" on the destination server.

Sample Scenario

This topic shows you how to use various parameters to achieve the following workflow export scenarios in your environment when using ["Promote Workflow – Export"](#).

Scenario 1: Export All Automation Items to a ZIP File

In this scenario, all deployments, Smart Groups, and Custom Fields that are referenced by the workflow (or any of its deployments) are exported. The XML files will be stored in the specified Export Location on the target server.

Example Parameter Values for Gather Parameters for Promote Workflow – Export

Parameter Name	Example	Description
Export Location	/Oracle Workflows/workflow123.zip	The location where the exported DMA artifacts are stored. This can be either a fully qualified ZIP filename (default) or a fully qualified directory path—based on the advanced parameter Export Zip Archive. If it is a directory, a time-stamped sub-directory or ZIP file will be created to store the files. The location is on the target server.
Workflow Name	Run Oracle Compliance Check - CIS	Name of the workflow to be promoted.

Be sure that the default values for all remaining input parameters are appropriate for your environment (see ["Parameters for Promote Workflow – Export" on page 1464](#)).

Scenario 2: Export All Automation Items to a Sub-Directory

In this scenario, all deployments, Smart Groups, and Custom Fields that are referenced by the workflow (or any of its deployments) are exported. The XML files will be stored in the specified Export Location on the target server.

Example Parameter Values for Gather Parameters for Promote Workflow – Export

Parameter Name	Example	Description
Export Location	/Oracle Workflows	The location where the exported DMA artifacts are stored. This can be either a fully qualified ZIP filename (default) or a fully qualified directory path—based on the advanced parameter Export Zip Archive. If it is a directory, a time-stamped sub-directory or ZIP file will be created to store the files. The location is on the target server.
Workflow Name	Run Oracle Compliance Check - CIS	Name of the workflow to be promoted.

The following parameter is not visible by default in a deployment. You need to expose it before you can use it.

Example Parameter Values for Gather Advanced Parameters for Promote Workflow – Export

Parameter Name	Example	Description
Export Zip Archive	NO	Flag to indicate whether the workflow (and related automation items) and log files are exported as a ZIP file. If set to YES or TRUE (the default), the files are exported to a ZIP file. If set to NO or FALSE, the files are exported to a time-stamped sub-directory of the Export Location.

Be sure that the default values for all remaining input parameters are appropriate for your environment (see ["Parameters for Promote Workflow – Export" on the next page](#)).

Parameters for Promote Workflow – Export

The following tables describe the required and optional input parameters for this workflow. For some parameters, if you do not specify a value for a parameter, a default value is assigned.

Input Parameters Defined in this Step: Gather Parameters for Promote Workflow – Export

Parameter Name	Default Value	Required	Description
Export Location	no default	required	The location where the exported DMA artifacts are stored. This can be either a fully qualified ZIP filename (default) or a fully qualified directory path—based on the advanced parameter Export Zip Archive. If it is a directory, a time-stamped sub-directory or ZIP file will be created to store the files. The location is on the target server.
Workflow Name	no default	required	Name of the workflow to be promoted.

The following parameter is not visible by default in a deployment. You need to expose it before you can use it.

Additional Input Parameters Defined in this Step: Gather Advanced Parameters for Promote Workflow - Export

Parameter Name	Default Value	Required	Description
Filter Deployments	INCLUDE: Run Oracle Compliance Check - CIS - Linux Svrs	<p>Comma-separated list of deployments that will be exported from the source server.</p> <p>If this parameter is blank, all deployments associated with the specified workflow will be exported.</p> <p>Note: Maximum number of characters is 1000.</p>	Filter Deployments

Promote Workflow – Import

To use this workflow in your environment, see the following information:

Topic	Information Included
"Prerequisites for this Workflow"	List of prerequisites that must be satisfied before you can run this workflow
"How This Workflow Works"	Information about what the workflow does, including validation checks performed, and steps executed
"How to Run This Workflow"	Instructions for running this workflow in your environment
"Sample Scenarios"	Examples of typical parameter values for this workflow
Parameters	List of input parameters for this workflow

The information presented here assumes the following:

- DMA is installed and operational.
- At least one suitable target server is available.
- You are logged in to DMA as a user with Workflow Creator (or Administrator) capability.
- You have Read and Execute permission for the organization that contains your target server.

Prerequisites for this Workflow

Be sure that the following prerequisites are satisfied before you run the ["Promote Workflow – Import"](#) workflow:

- You are using Database and Middleware Automation version 10.50 (or later).
- You have installed the latest version of the Promote Solution Pack.
- Any roles required to modify or execute the workflow (or workflows) that will be promoted must exist on the destination DMA server.
- The DMA user who runs the workflow should have READ and WRITE permissions on the promoted objects.
- The DMA user who runs the workflow must have Administrator capability.

Before you run ["Promote Workflow – Import"](#), you must have access to your exported workflow that was created when you ran either of the following:

- ["Promote Workflow – Export"](#)
- ["Promote Workflow – Export and Import"](#)

How This Workflow Works

"[Promote Workflow – Import](#)" copies a workflow and related automation items to the DMA server where you run the workflow (the destination). This workflow consumes the collection of previously created XML files that contain the workflow and its related automation items.

Normally, you run "[Promote Workflow – Export](#)" before you run "[Promote Workflow – Import](#)" to produce the XML files.

By using these two workflows together, you can promote a customized workflow and all its components from one DMA server (the source) to another DMA server (the destination) in a reliable and replicable manner. This is useful, for example, when you want to move a workflow from a test environment to a production environment.



For a list of the specific items exported, see [What is Promoted](#).

Tip: You can use the preview mode to see what will be promoted to the destination server. In preview mode, no changes are made to the destination server.

Process Flow

There are five phases included in the Promote Workflow - Import process flow.

Phase	Purpose	Artifacts Created
1	Compare the XML files to the workflow on the destination server (if the workflow already exists there).	objects_to_promote.txt promote_summary.txt
2	Back up the workflow on the destination server (if the workflow already exists there).	Destination backup files
3	Import the workflow to the destination server.	none
4	Validate the promoted workflow on the destination server.	none
5	If the promotion failed or cannot be validated, roll back the original version of the workflow on the destination server.	none

Note: If the Preview Only parameter is set to YES, only Phase 1 in this process is performed.

Steps Executed

Promote Workflow – Import includes the following steps. Each step must complete successfully before the next step can start. If a step fails, the workflow reports a failure and all subsequent steps are skipped.

Steps Used in Promote Workflow - Import

Workflow Step	Description
Gather Parameters for Promote Workflow – Import	Gets the preview mode setting (whether the promote operation only previews the changes without updating the destination server), the roles, the Import Location, and the filters for Deployments, Policies, and Smart Groups to promote.
Gather Advanced Parameters for Promote Workflow – Import	Gets the advanced optional parameters: Email Address that specifies optional email addresses where a summary report will be sent, Ignore Platform Version setting that specifies whether to ignore a difference in the source server version and the destination server version, and Rollback on Error setting that tells DMA what to do if the promote fails—if YES, rolls back the existing workflow (if any) on the destination server; if NO, does not roll back.
Validate Parameters for Promote Workflow – Import	<p>Verifies the following:</p> <ul style="list-style-type: none"> • All required parameters have been specified. • The specified role exists on the destination server. • The specified Import Location exists and contains the DMA exported XML files. • The source server version matches the destination server version—unless Ignore Platform Version is YES.
Preview Promote	<p>The Preview Promote step looks for any conflicts that may arise as a result of the promote operation. The step reads each XML file in the working directory/ZIP file that contains an exported item (file name begins with <code>source_</code>) and performs the following checks:</p> <ul style="list-style-type: none"> • It determines which deployments, policies, and Smart Groups to promote based on the filter parameters: Filter Deployments, Filter Smart Groups, and Filter Policies. • It identifies any exported policy attributes or parameters that represent passwords and prints a warning to the step log indicating that these items must be manually configured on the destination server after the promote operation is completed. If the password exists on the destination, the value will be preserved. • It determines whether an item with the same name and target level (if applicable) as the exported item already exists on the destination server. <p>If an exported item exists on the destination server, the step compares the exported item to the destination item. The following summarizes the action taken based on the result of this comparison:</p> <p>Identical Item does not need to be imported to the destination server.</p> <p>Not identical The Preview Promote step logs a list of items that will be promoted in the file <code>objects_to_promote.txt</code> in the Import Location.</p> <p>Note: Locked items are not overwritten. If a step or function is locked and is different on the destination server, then the version of the solution pack used during the Promote export does not match the solution pack version on your destination server. The promote will fail.</p> <ul style="list-style-type: none"> • It lists any items on the destination server that have dependencies on the existing item in the step log. • It creates the file <code>objects_to_promote.txt</code> that contains the automation items

Steps Used in Promote Workflow - Import, continued

Workflow Step	Description
	<p>that will be promoted.</p> <ul style="list-style-type: none"> It creates a Preview report (<code>promote_summary.txt</code>). The Preview report lists what will be promoted and describes what you need to do after running the Promote workflows such as setting up passwords and Custom Fields. <p>Note: If you are running the workflow in preview mode (parameter Preview Only is set to YES), the workflow stops after this step.</p>
Import Objects to Destination Server	<p>This step (and the following steps) are only executed if Preview Only is set to NO.</p> <p>Reads the XML files containing the exported workflow, backs up the workflow and the specified (filtered) related automation items, and then creates the items on the destination server.</p> <p>Caution: The workflow and automation items that previously existed on the destination server will be over-written.</p>
Post Verification Promote	<p>The Post Verification Promote step is executed after the workflow and all related items are imported to the destination server to ensure that the promote operation was successful. In this case, all source items and destination items should be identical. Items that are unique to the destination environment, such as passwords, are ignored.</p> <p>If this comparison determines that the promoted workflow and all related items match the source workflow, the workflow ends in with a Success state.</p> <p>If this comparison determines that the promoted workflow and all related items do not match the source workflow:</p> <ol style="list-style-type: none"> If Rollback on Error is set to YES: The workflow runs the Rollback Objects on Destination Server and Verify Rollback steps. The workflow ends in a Failure state.
Send Promote Summary	<p>If Email Address is specified, this step emails a Promote summary for the successful promotion.</p>
Rollback Objects on Destination Server	<p>This step is only executed if the promote operation fails and Rollback on Error is set to YES:</p> <ul style="list-style-type: none"> If a previous version of the promoted workflow (or any related automation item) existed on the destination server prior to the promote operation: Deletes the promoted workflow (or related item) on the destination server, and restores the original workflow or related automation item to the item that was previously backed up (file names begin with <code>backup_</code>). If no previous version of the promoted workflow (or any related automation item) existed on the destination server prior to the promote operation: The workflow (or related automation item) will be deleted from the destination server.
Verify Rollback	<p>The Verify Rollback step is only executed if a rollback is performed. For the workflow and all related automation items, the step checks the following:</p> <ul style="list-style-type: none"> If the item was rolled back, the restored item on the destination server should be identical to the version of that item that was previously backed up (file names begin with <code>backup_</code>).

Steps Used in Promote Workflow - Import, continued

Workflow Step	Description
	<ul style="list-style-type: none">• If the item did not exist before the promotion, the item does not exist after the roll back.
Send Promote Summary	If Email Address is specified, this step emails a Promote summary after a rollback occurs.

Note: For input parameter descriptions and defaults, see "[Parameters for Promote Workflow – Import](#)" on page 1481.

How to Run This Workflow

The following instructions show you how to customize and run "[Promote Workflow – Import](#)" in your environment. These instructions assume that all deployments, Smart Groups, and Custom Fields will be promoted.

Note: Before following this procedure, review the "[Prerequisites for this Workflow](#)" on page 1466, and ensure that all requirements are satisfied.

Tip: As a best practice, set the target for the deployment to the DMA server where you run "[Promote Workflow – Import](#)".

To use the Promote Workflow – Import workflow:

1. On the DMA server where you run the workflow, create a deployable copy of the workflow.
2. Determine the values that you will specify for the following parameters: show

Input Parameters for Gather Parameters for Promote Workflow - Import

Parameter Name	Default Value	Required	Description
Filter Deployments	ALL	required	<p>A filter for deployments to be promoted. Valid values are ALL, NONE, INCLUDE: followed by a comma separated list of deployments to include, or EXCLUDE: followed by a comma separated list of deployments to exclude. The value ALL will promote all deployments associated with the workflow; the value NONE will not promote any of the deployments associated with the workflow.</p> <p>Note: Maximum number of characters is 1000.</p>
Filter Policies	ALL	required	<p>A filter for policies to be promoted. Valid values are ALL, NONE, INCLUDE: followed by a comma separated list of policies to include, or EXCLUDE: followed by a comma separated list of policies to exclude. The value ALL will promote all policies associated with the workflow; the value NONE will not promote any of the policies associated with the workflow.</p> <p>Note: Maximum number of characters is 1000.</p>
Filter Smart Groups	ALL	required	<p>A filter for Smart Groups to be promoted. Valid values are ALL, NONE, INCLUDE: followed by a comma separated list of Smart Groups to include, or EXCLUDE: followed by a comma separated list of Smart Groups to exclude. The value ALL will promote all Smart Groups associated with the workflow; the value NONE will not promote any of the Smart Groups associated with the workflow.</p> <p>Note: Maximum number of characters is 1000.</p>

Input Parameters for Gather Parameters for Promote Workflow - Import, continued

Parameter Name	Default Value	Required	Description								
Import Location	no default	required	The location on the target server where all export files generated by Promote workflow are stored. If you use the same location where Promote Workflow - Export generated the files, include the /promote_<workflow_name>_<date>_<time> sub-directory/zip-archive in the path.								
Preview Only	YES	required	If Preview Only is set to YES, the workflow will show you which items will be promoted, but it will not make any changes on the destination server. Valid values are YES/TRUE and NO/FALSE (case-insensitive).								
Roles on Destination Server	no default	required	<p>Comma-separated list of roles that will be assigned to promoted items. At least one role must be specified.</p> <p>All roles are assigned to the following promoted items (workflows, steps, deployments, and policies) that do not exist on the destination DMA server prior to the promote operation. The roles specified for these promoted items are given full permissions:</p> <table><tr><td>Workflow</td><td>READ, WRITE</td></tr><tr><td>Step</td><td>READ, WRITE</td></tr><tr><td>Deployment</td><td>READ, WRITE, EXECUTE</td></tr><tr><td>Policy</td><td>READ, WRITE</td></tr></table> <p>The first role specified in Roles on Destination Server is set in the Roles attribute for promoted Smart Groups that do not exist on the destination server prior to the promote operation.</p> <p>Role-based permissions for existing items are preserved.</p> <p>Note: If the roles do not yet exist on the destination server, you need to create them before attempting to promote.</p>	Workflow	READ, WRITE	Step	READ, WRITE	Deployment	READ, WRITE, EXECUTE	Policy	READ, WRITE
Workflow	READ, WRITE										
Step	READ, WRITE										
Deployment	READ, WRITE, EXECUTE										
Policy	READ, WRITE										

Note: This is the minimum set of parameters required to run this workflow. You may want to specify additional parameters depending on your objectives.

See ["Parameters for Promote Workflow – Import" on page 1481](#) for detailed descriptions of all input parameters for this workflow, including default values.

3. Create a new deployment.
4. On the Parameters tab, specify values for the required parameters listed in step 2. You do not need to specify values for those parameters whose default values are appropriate for your environment.

5. On the Targets tab, specify a target for this deployment—where the exported workflow (and all related items) and the log files are stored.

Tip: As a best practice, copy the exported working directory/ZIP file to the DMA server where you run the workflow (the destination) and set the target to the DMA to the same server.

6. Save the deployment (click **Save** in the lower right corner).
7. Run the workflow using this deployment.

To verify the results:

The workflow will complete and report SUCCESS on the Console if it has run successfully. If an error occurs during workflow execution, the error is logged, and the workflow terminates in the FAILURE state.

Results of each step are logged on the Output tab for each step. You can access this information from the Console page while the workflow is running or the History page after it finishes running.

Tip: Examine the Output tab for any dependencies (for example, other workflows that use the promoted steps or functions) and decide if any other promotions are desired.

You should examine the Preview report in file `promote_summary.txt` to determine what objects were promoted and exactly what needs to be customized on the destination server.

To track the history of promoted items on the destination server:

You can track the history of promoted workflows, steps, and functions using the history tab:

Promoted Item	How to Access	Description
Workflow	Automation > Workflows > <i><promoted_workflow></i> > History	Date: <i><date_time_of_promotion></i> Person: <i><user_that_promoted_workflow></i> Source: REST API Comment: Promoted using " <i><promote_workflow_that_imported_item></i> " from DMA server <i><server_name></i>
Step	Automation > Steps > <i><promoted_step></i> > History	Date: <i><date_time_of_promotion></i> Person: <i><user_that_promoted_step></i> Source: REST API Comment: Promoted with " <i><promoted_workflow></i> "
Function	Automation > Functions > <i><promoted_function></i> > History	Date: <i><date_time_of_promotion></i> Person: <i><user_that_promoted_function></i> Source: REST API Comment: Promoted with " <i><promoted_workflow></i> "

To use the promoted workflow on the destination server:

Before you run the newly promoted workflow, use the Preview report (file `promote_summary.txt`) to customize the following on the destination server:

- Password values
- Custom Field values

Set up the environment on the destination server:

- Environments: organizations, servers, instances, and databases
- Targets for deployments

Sample Scenarios

This topic shows you how to use various parameters to achieve the following workflow promotion scenarios in your environment when using ["Promote Workflow – Import"](#).

Scenario 1: Preview All Automation Items but Do Not Import

In this scenario, all automation items for the specified workflow that are stored in Import Location are previewed. They are not created or updated on the destination server.

In this scenario, Preview Only is enabled by default.

In this scenario, Rollback on Error is enabled by default. The workflow and any related items that existed on the destination server prior to the promote operation will be restored in the event that the promote fails.

Example Parameter Values for Gather Parameters for Promote Workflow – Import

Parameter Name	Example	Description								
Import Location	/Oracle Workflows/workflow123.zip	The location on the target server where all export files generated by Promote workflow are stored. If you use the same location where Promote Workflow - Export generated the files, include the /promote_<workflow_name>_<date>_<time> sub-directory/zip-archive in the path.								
Roles on Destination Server	DMA Admins	<p>Comma-separated list of roles that will be assigned to promoted items. At least one role must be specified.</p> <p>All roles are assigned to the following promoted items (workflows, steps, deployments, and policies) that do not exist on the destination DMA server prior to the promote operation. The roles specified for these promoted items are given full permissions:</p> <table><tr><td>Workflow</td><td>READ, WRITE</td></tr><tr><td>Step</td><td>READ, WRITE</td></tr><tr><td>Deployment</td><td>READ, WRITE, EXECUTE</td></tr><tr><td>Policy</td><td>READ, WRITE</td></tr></table> <p>The <u>first</u> role specified in Roles on Destination Server is set in the Roles attribute for promoted Smart Groups that do not exist on the destination server prior to the promote operation.</p> <p>Role-based permissions for existing items are preserved.</p> <p>Note: If the roles do not yet exist on the destination server, you need to create them before attempting to promote.</p>	Workflow	READ, WRITE	Step	READ, WRITE	Deployment	READ, WRITE, EXECUTE	Policy	READ, WRITE
Workflow	READ, WRITE									
Step	READ, WRITE									
Deployment	READ, WRITE, EXECUTE									
Policy	READ, WRITE									

Be sure that the default values for all remaining input parameters are appropriate for your environment (see ["Parameters for Promote Workflow – Import"](#) on page 1481).

Scenario 2: Import All Automation Items

In this scenario, all automation items for the specified workflow that are stored in Import Location are created or updated on the destination server. The Database Compliance summary report will be emailed to a recipient.

In this scenario, Rollback on Error is enabled by default. The workflow and any related items that existed on the destination server prior to the promote operation will be restored in the event that the promote fails.

Example Parameter Values for Gather Parameters for Promote Workflow – Import

Parameter Name	Example	Description								
Import Location	/Oracle Workflows/workflow123.zip	The location on the target server where all export files generated by Promote workflow are stored. If you use the same location where Promote Workflow - Export generated the files, include the /promote_<workflow_name>_<date>_<time> sub-directory/zip-archive in the path.								
Preview Only	NO	If Preview Only is set to YES, the workflow will show you which items will be promoted, but it will not make any changes on the destination server. Valid values are YES/TRUE and NO/FALSE (case-insensitive).								
Roles on Destination Server	DMA Admins	<p>Comma-separated list of roles that will be assigned to promoted items. At least one role must be specified.</p> <p>All roles are assigned to the following promoted items (workflows, steps, deployments, and policies) that do not exist on the destination DMA server prior to the promote operation. The roles specified for these promoted items are given full permissions:</p> <table><tr><td>Workflow</td><td>READ, WRITE</td></tr><tr><td>Step</td><td>READ, WRITE</td></tr><tr><td>Deployment</td><td>READ, WRITE, EXECUTE</td></tr><tr><td>Policy</td><td>READ, WRITE</td></tr></table> <p>The <u>first</u> role specified in Roles on Destination Server is set in the Roles attribute for promoted Smart Groups that do not exist on the destination server prior to the promote operation.</p> <p>Role-based permissions for existing items are preserved.</p> <p>Note: If the roles do not yet exist on the destination server, you need to create them before attempting to promote.</p>	Workflow	READ, WRITE	Step	READ, WRITE	Deployment	READ, WRITE, EXECUTE	Policy	READ, WRITE
Workflow	READ, WRITE									
Step	READ, WRITE									
Deployment	READ, WRITE, EXECUTE									
Policy	READ, WRITE									

The following parameter is not visible by default in a deployment. You need to expose it before you can use it.

Example Parameter Values for Gather Advanced Parameters for Promote Workflow - Import

Parameter Name	Example	Description
Email Address	JohnDoe@mycompany.com	Comma separated list of email addresses where the Database Compliance summary report will be sent.

Be sure that the default values for all remaining input parameters are appropriate for your environment (see ["Parameters for Promote Workflow – Import" on page 1481](#)).

Scenario 3: Import Only a Subset of Deployments, Policies, and Smart Groups

In this scenario, the deployments, policies, and Smart Groups to be promoted are specifically included or excluded.

- Included objects: Provided that these objects are referenced by the specified workflow or one (or more) of its deployments, the objects will be created or updated on the destination server. Any objects that are not explicitly specified will be not be promoted.
- Excluded objects: All objects that are not in the exclude list and are referenced by the specified workflow or one (or more) of its deployments, the objects will be created or updated on the destination server.

In this scenario, Preview Only is set to NO.

In this scenario, Rollback on Error is enabled by default. The workflow and any related items that existed on the destination server prior to the promote operation will be restored in the event that the promote fails.

Example Parameter Values for Gather Parameters for Promote Workflow – Import

Parameter Name	Example	Description
Filter Deployments	INCLUDE: Run Oracle Compliance Check - CIS - Linux Svrs	<p>A filter for deployments to be promoted. Valid values are ALL, NONE, INCLUDE: followed by a comma separated list of deployments to include, or EXCLUDE: followed by a comma separated list of deployments to exclude. The value ALL will promote all deployments associated with the workflow; the value NONE will not promote any of the deployments associated with the workflow.</p> <p>Note: Maximum number of characters is 1000.</p>
Filter Policies	EXCLUDE: Oracle Test Compliance	<p>A filter for policies to be promoted. Valid values are ALL, NONE, INCLUDE: followed by a comma separated list of policies to include, or EXCLUDE: followed by a comma separated list of policies to exclude. The value ALL will promote all policies associated with the workflow; the value NONE will not promote any of the policies associated with the workflow.</p> <p>Note: Maximum number of characters is 1000.</p>
Filter Smart Groups	INCLUDE: Linux Svrs, Europe Svrs	<p>A filter for Smart Groups to be promoted. Valid values are ALL, NONE, INCLUDE: followed by a comma separated list of Smart Groups to include, or EXCLUDE: followed by a comma separated list of Smart Groups to exclude. The value ALL will promote all Smart Groups associated with the workflow; the value NONE will not promote any of the Smart Groups associated with the workflow.</p> <p>Note: Maximum number of characters is 1000.</p>
Import	/Oracle	The location on the target server where all export files generated

Example Parameter Values for Gather Parameters for Promote Workflow – Import, continued

Parameter Name	Example	Description								
Location	Workflows/ workflow123.zip	by Promote workflow are stored. If you use the same location where Promote Workflow - Export generated the files, include the /promote_<workflow_name>_<date>_<time> sub-directory/zip-archive in the path.								
Preview Only	NO	If Preview Only is set to YES, the workflow will show you which items will be promoted, but it will not make any changes on the destination server. Valid values are YES/TRUE and NO/FALSE (case-insensitive).								
Roles on Destination Server	DMA Admins	<p>Comma-separated list of roles that will be assigned to promoted items. At least one role must be specified.</p> <p>All roles are assigned to the following promoted items (workflows, steps, deployments, and policies) that do not exist on the destination DMA server prior to the promote operation. The roles specified for these promoted items are given full permissions:</p> <table><tr><td>Workflow</td><td>READ, WRITE</td></tr><tr><td>Step</td><td>READ, WRITE</td></tr><tr><td>Deployment</td><td>READ, WRITE, EXECUTE</td></tr><tr><td>Policy</td><td>READ, WRITE</td></tr></table> <p>The first role specified in Roles on Destination Server is set in the Roles attribute for promoted Smart Groups that do not exist on the destination server prior to the promote operation.</p> <p>Role-based permissions for existing items are preserved.</p> <p>Note: If the roles do not yet exist on the destination server, you need to create them before attempting to promote.</p>	Workflow	READ, WRITE	Step	READ, WRITE	Deployment	READ, WRITE, EXECUTE	Policy	READ, WRITE
Workflow	READ, WRITE									
Step	READ, WRITE									
Deployment	READ, WRITE, EXECUTE									
Policy	READ, WRITE									

Be sure that the default values for all remaining input parameters are appropriate for your environment (see ["Parameters for Promote Workflow – Import" on the next page](#)).

Parameters for Promote Workflow – Import

The following tables describe the required and optional input parameters for this workflow. For some parameters, if you do not specify a value for a parameter, a default value is assigned.

Input Parameters Defined in this Step: Gather Parameters for Promote Workflow - Import

Parameter Name	Default Value	Required	Description
Filter Deployments	ALL	required	<p>A filter for deployments to be promoted. Valid values are ALL, NONE, INCLUDE: followed by a comma separated list of deployments to include, or EXCLUDE: followed by a comma separated list of deployments to exclude. The value ALL will promote all deployments associated with the workflow; the value NONE will not promote any of the deployments associated with the workflow.</p> <p>Note: Maximum number of characters is 1000.</p>
Filter Policies	ALL	required	<p>A filter for policies to be promoted. Valid values are ALL, NONE, INCLUDE: followed by a comma separated list of policies to include, or EXCLUDE: followed by a comma separated list of policies to exclude. The value ALL will promote all policies associated with the workflow; the value NONE will not promote any of the policies associated with the workflow.</p> <p>Note: Maximum number of characters is 1000.</p>
Filter Smart Groups	ALL	required	<p>A filter for Smart Groups to be promoted. Valid values are ALL, NONE, INCLUDE: followed by a comma separated list of Smart Groups to include, or EXCLUDE: followed by a comma separated list of Smart Groups to exclude. The value ALL will promote all Smart Groups associated with the workflow; the value NONE will not promote any of the Smart Groups associated with the workflow.</p> <p>Note: Maximum number of characters is 1000.</p>
Import Location	no default	required	<p>The location on the target server where all export files generated by Promote workflow are stored. If you use the same location where Promote Workflow - Export generated the files, include the /promote_<workflow_name>_<date>_<time> sub-directory/zip-archive in the path.</p>
Preview Only	YES	required	<p>If Preview Only is set to YES, the workflow will show you which items will be promoted, but it will not make any changes on the destination server. Valid values are YES/TRUE and NO/FALSE (case-insensitive).</p>
Roles on Destination Server	no default	required	<p>Comma-separated list of roles that will be assigned to promoted items. At least one role must be specified.</p> <p>All roles are assigned to the following promoted items (workflows, steps, deployments, and policies) that do not exist on the destination DMA server prior to the promote operation. The roles specified for these promoted items are</p>

Input Parameters Defined in this Step: Gather Parameters for Promote Workflow - Import, continued

Parameter Name	Default Value	Required	Description								
			<p>given full permissions:</p> <table><tr><td>Workflow</td><td>READ, WRITE</td></tr><tr><td>Step</td><td>READ, WRITE</td></tr><tr><td>Deployment</td><td>READ, WRITE, EXECUTE</td></tr><tr><td>Policy</td><td>READ, WRITE</td></tr></table> <p>The first role specified in Roles on Destination Server is set in the Roles attribute for promoted Smart Groups that do not exist on the destination server prior to the promote operation.</p> <p>Role-based permissions for existing items are preserved.</p> <p>Note: If the roles do not yet exist on the destination server, you need to create them before attempting to promote.</p>	Workflow	READ, WRITE	Step	READ, WRITE	Deployment	READ, WRITE, EXECUTE	Policy	READ, WRITE
Workflow	READ, WRITE										
Step	READ, WRITE										
Deployment	READ, WRITE, EXECUTE										
Policy	READ, WRITE										

The following parameters are not visible by default in a deployment. You need to expose them before you can use them.

Additional Input Parameters Defined in this Step: Gather Advanced Parameters for Promote Workflow - Import

Parameter Name	Default Value	Required	Description
Email Address	no default	optional	Comma separated list of email addresses where the Database Compliance summary report will be sent.
Ignore Platform Version	NO	optional	<p>If set to NO (default), the Database Compliance workflows check that the source and destination DMA platform versions are the same. If set to YES, the Database Compliance workflows ignore different DMA platform versions and will attempt to promote the workflow anyway. Valid values are YES/TRUE and NO/FALSE (case-insensitive).</p> <p>Caution: Promote does not officially support promoting between different versions. Use at your own risk.</p>
Rollback on Error	YES	optional	Set to NO if you do NOT want DMA to rollback the workflow and all related items on the destination server to their original state in the event that the promote operation fails. Valid values are YES/TRUE and NO/FALSE (case-insensitive).

Promote Workflow – Export and Import

The Promote Workflow workflow enables you to promote (copy) a customized workflow and all related items from one DMA server (the source) to another DMA server (the destination) in a reliable and replicable manner. This is useful, for example, when you want to move a workflow from a test environment to a production environment.



The functionality is the same as running the "Promote Workflow – Export" workflow followed by running the "Promote Workflow – Import" workflow.



Note: This workflow requires that the SSL certificates are configured the same on the two servers. The `com.hp.dma.conn.trustAllCertificates` parameter in both servers' `dma.xml` files must have the same values. If the DMA source server does not trust all SSL certificates but the DMA destination server does, then you need to first run "Promote Workflow – Export", and then run "Promote Workflow – Import".

To run the Database Compliance workflow, use the information found in the following workflows:

- "Promote Workflow – Export"
- "Promote Workflow – Import"

Tip: You can use the preview mode to see what will be copied to the destination server. In preview mode, no changes are made to the destination server.

Process Flow

1. Export Process

First, the workflow exports the specified workflow and the related automation items from the DMA source server, and stores this information in a collection of XML files in the Export Location.

The export process creates the `promote_info.txt` file.

2. Import Process

After the workflow exports the specified workflow and the related automation items to a collection of XML files, the workflow imports them to the destination server. There are five phases included in the import process flow.

Phase	Purpose	Artifacts Created
1	Compare the XML files to the workflow on the destination server (if the workflow already exists there).	objects_to_promote.txt promote_summary.txt
2	Back up the workflow on the destination server (if the workflow already exists there).	Destination backup files
3	Import the workflow to the destination server.	
4	Validate the promoted workflow on the destination server.	none
5	If the promotion failed or cannot be validated, roll back the original version of the workflow on the destination server.	none

Note: If the Preview Only parameter is set to YES, only Phase 1 in this process is performed.

To use this workflow in your environment, see the following information:

Topic	Information Included
"Prerequisites for this Workflow"	List of prerequisites that must be satisfied before you can run this workflow
"How This Workflow Works"	Information about what the workflow does, including validation checks performed, and steps executed
"How to Run This Workflow"	Instructions for running this workflow in your environment
"Sample Scenarios"	Examples of typical parameter values for this workflow
Parameters	List of input parameters for this workflow

The information presented here assumes the following:

- DMA is installed and operational.
- At least one suitable target server is available.
- You are logged in to DMA as a user with Workflow Creator (or Administrator) capability.
- You have Read and Execute permission for the organization that contains your target server.

Prerequisites for this Workflow

Be sure that the following prerequisites are satisfied before you run "[Promote Workflow – Export and Import](#)":

- You are using Database and Middleware Automation version 10.50 (or later).
- You have installed the latest version of the Database Compliance Solution Pack.
- Any roles required to modify or execute the workflow (or workflows) that will be promoted must exist on the destination DMA server.
- The DMA user who runs the workflow should have READ and WRITE permissions on the promoted objects.
- The DMA user specified in the Destination DMA Username parameter must have Administrator capability.

How This Workflow Works

"Promote Workflow – Export and Import" enables you to copy a customized workflow and all related items from the DMA server where you run the workflow (the source) to another DMA server (the destination) in a reliable and replicable manner. This is useful, for example, when you want to move a workflow from a development environment to a developer's test environment where no proxy exists between the two environments.



Tip: You can use the preview mode to see what will be copied to the destination server. In preview mode, no changes are made to the destination server.

Process Flow

1. Export Process

First, the workflow exports the specified workflow and the related automation items from the DMA source server, and stores this information in a collection of XML files in the Export Location.

The export process creates the `promote_info.txt` file.

2. Import Process

After the workflow exports the specified workflow and the related automation items to a collection of XML files, the workflow imports them to the destination server. There are five phases included in the import process flow.

Phase	Purpose	Artifacts Created
1	Compare the XML files to the workflow on the destination server (if the workflow already exists there).	objects_to_promote.txt promote_summary.txt

Phase	Purpose	Artifacts Created
2	Back up the workflow on the destination server (if the workflow already exists there).	Destination backup files
3	Import the workflow to the destination server.	none
4	Validate the promoted workflow on the destination server.	none
5	If the promotion failed or cannot be validated, roll back the original version of the workflow on the destination server.	none

Note: If the Preview Only parameter is set to YES, only Phase 1 in this process is performed.

Steps Executed

Promote Workflow - Export and Import includes the following steps. Each step must complete successfully before the next step can start. If a step fails, the workflow reports a failure and all subsequent steps are skipped.

Steps Used in Promote Workflow - Export and Import

Workflow Step	Description
Gather Parameters for Promote Workflow	Gets the destination server information, whether the workflow is to run in preview mode (without updating the destination server), the roles, the name of the workflow to be promoted, and the filters for Deployments, Policies, and Smart Groups to promote. Sets the working directory/ZIP file.
Gather Advanced Parameters for Promote Workflow	Gets the advanced optional parameters: Email Address that specifies optional email addresses where a summary report will be sent, Export Zip Archive setting that specifies whether to export the workflow and related automation items as a ZIP archive or a sub-directory, Ignore Platform Version setting that specifies whether to ignore a difference in the source server version and the destination server version, and Rollback on Error setting that tells DMA what to do if the promote fails—if YES, rolls back the existing workflow (if any) on the destination server; if NO, does not roll back.
Validate Parameters for Promote Workflow	Verifies the following: <ul style="list-style-type: none"> • All required parameters have been specified. • DMA can communicate with the specified destination server. • The specified workflow exists on the source server. • The specified roles exist on the destination server. • The source server version matches the destination server version—unless Ignore Platform Version is YES.
Export Objects from Source Server	Exports the workflow and the related automation items from the DMA source server, and stores this information in a collection of XML files in the working directory/ZIP file. Exports in the following order: <ol style="list-style-type: none"> 1. The workflow, itself 2. Steps used in the workflow 3. Functions referenced by steps used in the workflow 4. Deployments associated with the workflow 5. Policies associated with any promoted deployment 6. Smart Groups associated with any promoted deployment 7. Custom Fields that are referenced by the workflow, any promoted deployment, any promoted step, or any promoted Smart Group <p>Creates the <code>promote_info.txt</code> file.</p>
Preview Promote	The Preview Promote step looks for any conflicts that may arise as a result of the promote operation. The step reads each XML file in the working directory/ZIP file that contains an exported item (file name begins with <code>source_</code>) and performs the following checks: <ul style="list-style-type: none"> • It determines which deployments, policies, and Smart Groups to promote based on the filter parameters: Filter Deployments, Filter Smart Groups, and Filter Policies. • It identifies any exported policy attributes or parameters that represent passwords and prints a warning to the step log indicating that these items must be manually configured on the destination server after the promote operation is completed. If the password exists on the destination, the value will be preserved. • It determines whether an item with the same name and target level (if applicable)

Steps Used in Promote Workflow - Export and Import, continued

Workflow Step	Description
	<p>as the exported item already exists on the destination server.</p> <p>If an exported item exists on the destination server, the step compares the exported item to the destination item. The following summarizes the action taken based on the result of this comparison:</p> <p>Identical Item does not need to be imported to the destination server.</p> <p>Not identical The Preview Promote step logs a list of items that will be promoted in the file <code>objects_to_promote.txt</code> in the Import Location.</p> <p>Note: Locked items are not overwritten. If a step or function is locked and is different on the destination server, then the version of the solution pack used during the Promote export does not match the solution pack version on your destination server. The promote will fail.</p> <ul style="list-style-type: none"> • It lists any items on the destination server that have dependencies on the existing item in the step log. • It creates the file <code>objects_to_promote.txt</code> that contains the automation items that will be promoted. • It creates a Preview report (<code>promote_summary.txt</code>). The Preview report lists what will be promoted and describes what you need to do after running the Database Compliance workflows such as setting up passwords and Custom Fields. <p>Note: If you are running the workflow in preview mode (parameter Preview Only is set to YES), the workflow stops after this step.</p>
Import Objects to Destination Server	<p>This step (and the following steps) are only executed if Preview Only is set to NO.</p> <p>Reads the XML files containing the exported workflow, backs up the workflow and the specified (filtered) related automation items, and then creates the items on the destination server.</p> <p>Caution: The workflow and automation items that previously existed on the destination server will be over-written.</p>
Post Verification Promote	<p>The Post Verification Promote step is executed after the workflow and all related items are imported to the destination server to ensure that the promote operation was successful. In this case, all source items and destination items should be identical. Items that are unique to the destination environment, such as passwords, are ignored.</p> <p>If this comparison determines that the promoted workflow and all related items match the source workflow, the workflow ends in with a Success state.</p> <p>If this comparison determines that the promoted workflow and all related items do not match the source workflow:</p> <ol style="list-style-type: none"> 1. If Rollback on Error is set to YES: The workflow runs the Rollback Objects on Destination Server and Verify Rollback steps. 2. The workflow ends in a Failure state.
Rollback Objects on Destination	<p>This step is only executed if the promote operation fails and Rollback on Error is set to YES:</p>

Steps Used in Promote Workflow - Export and Import, continued

Workflow Step	Description
Server	<ul style="list-style-type: none"> • If a previous version of the promoted workflow (or any related automation item) existed on the destination server prior to the promote operation: Deletes the promoted workflow (or related item) on the destination server, and restores the original workflow or related automation item to the item that was previously backed up (file names begin with backup_). • If no previous version of the promoted workflow (or any related automation item) existed on the destination server prior to the promote operation: The workflow (or related automation item) will be deleted from the destination server.
Verify Rollback	<p>The Verify Rollback step is only executed if a rollback is performed. For the workflow and all related automation items, the step checks the following:</p> <ul style="list-style-type: none"> • If the item was rolled back, the restored item on the destination server should be identical to the version of that item that was previously backed up (file names begin with backup_). • If the item did not exist before the promotion, the item does not exist after the roll back.

Note: For input parameter descriptions and defaults, see "[Parameters for Promote Workflow - Export and Import](#)" on page 1502.

How to Run This Workflow

The following instructions show you how to run "[Promote Workflow – Export and Import](#)" in your environment. These instructions assume that all deployments, Smart Groups, and Custom Fields will be promoted.

Note: Before following this procedure, review the "[Prerequisites for this Workflow](#)" on page 1486, and ensure that all requirements are satisfied.

Tip: As a best practice, set the target for the deployment to the DMA server where you run "[Promote Workflow – Export and Import](#)", the same as the source server from which you are exporting the workflow and related automation.

To use the Promote Workflow workflow:

1. On the DMA server where you run the workflow, create a deployable copy of the workflow.
2. Determine the values that you will specify for the following parameters:

Input Parameters for Gather Parameters for Promote Workflow

Parameter Name	Default Value	Required	Description
Destination DMA Password	no default	required	Password for the user specified in the Destination DMA Username parameter.
Destination DMA URL	no default	required	URL for the destination DMA server. For example: <code>https://dma2.mycompany.com:8443/dma</code>
Destination DMA Username	no default	required	DMA user who will perform the promote operation on the destination server.
Export Location	no default	required	The location where the exported DMA artifacts are stored. This can be either a fully qualified ZIP filename (default) or a fully qualified directory path—based on the advanced parameter Export Zip Archive. If it is a directory, a time-stamped sub-directory or ZIP file will be created to store the files. The location is on the target server.
Filter Deployments	ALL	required	A filter for deployments to be promoted. Valid values are ALL, NONE, INCLUDE: followed by a comma separated list of deployments to include, or EXCLUDE: followed by a comma separated list of deployments to exclude. The value ALL will promote all deployments associated with the workflow; the value NONE will not promote any of the deployments associated with the workflow.

Input Parameters for Gather Parameters for Promote Workflow , continued

Parameter Name	Default Value	Required	Description								
			<div>Note: Maximum number of characters is 1000.</div>								
Filter Policies	ALL	required	<p>A filter for policies to be promoted. Valid values are ALL, NONE, INCLUDE: followed by a comma separated list of policies to include, or EXCLUDE: followed by a comma separated list of policies to exclude. The value ALL will promote all policies associated with the workflow; the value NONE will not promote any of the policies associated with the workflow.</p> <div>Note: Maximum number of characters is 1000.</div>								
Preview Only	YES	required	<p>If Preview Only is set to YES, the workflow will show you which items will be promoted, but it will not make any changes on the destination server. Valid values are YES/TRUE and NO/FALSE (case-insensitive).</p>								
Filter Smart Groups	ALL	required	<p>A filter for Smart Groups to be promoted. Valid values are ALL, NONE, INCLUDE: followed by a comma separated list of Smart Groups to include, or EXCLUDE: followed by a comma separated list of Smart Groups to exclude. The value ALL will promote all Smart Groups associated with the workflow; the value NONE will not promote any of the Smart Groups associated with the workflow.</p> <div>Note: Maximum number of characters is 1000.</div>								
Roles on Destination Server	no default	required	<p>Comma-separated list of roles that will be assigned to promoted items. At least one role must be specified.</p> <p>All roles are assigned to the following promoted items (workflows, steps, deployments, and policies) that do not exist on the destination DMA server prior to the promote operation. The roles specified for these promoted items are given full permissions:</p> <table><tr><td>Workflow</td><td>READ, WRITE</td></tr><tr><td>Step</td><td>READ, WRITE</td></tr><tr><td>Deployment</td><td>READ, WRITE, EXECUTE</td></tr><tr><td>Policy</td><td>READ, WRITE</td></tr></table> <p>The first role specified in Roles on Destination Server is set in the Roles attribute for promoted Smart Groups that do not exist on the destination server prior to the promote operation.</p> <p>Role-based permissions for existing items are preserved.</p> <div>Note: If the roles do not yet exist on the destination server, you need to create them before attempting to promote.</div>	Workflow	READ, WRITE	Step	READ, WRITE	Deployment	READ, WRITE, EXECUTE	Policy	READ, WRITE
Workflow	READ, WRITE										
Step	READ, WRITE										
Deployment	READ, WRITE, EXECUTE										
Policy	READ, WRITE										

Input Parameters for Gather Parameters for Promote Workflow , continued

Parameter Name	Default Value	Required	Description
Workflow Name	no default	required	Name of the workflow to be promoted.

Note: This is the minimum set of parameters required to run this workflow. You may want to specify other parameters depending on your objectives.

See ["Parameters for Promote Workflow - Export and Import" on page 1502](#) for detailed descriptions of all input parameters for this workflow, including default values.

3. Create a new deployment.
4. On the Parameters tab, specify values for the required parameters listed in step 2. You do not need to specify values for those parameters whose default values are appropriate for your environment.
5. On the Targets tab, specify a target for this deployment—where the exported workflow (and all related items) and the log files will be stored.

Tip: As a best practice, set the target to the DMA source server where the workflow is exported from.

6. Save the deployment (click **Save** in the lower right corner).
7. Run the workflow using this deployment.

To verify the results:

The workflow will complete and report SUCCESS on the Console if it has run successfully. If an error occurs during workflow execution, the error is logged, and the workflow terminates in the FAILURE state.

Results of each step are logged on the Output tab for each step. You can access this information from the Console page while the workflow is running or the History page after it finishes running.

Tip: Examine the Output tab for any dependencies (for example, other workflows that use the promoted steps or functions) and decide if any other promotions are desired.

You should examine the Preview report in file `promote_summary.txt` to determine what objects were promoted and exactly what needs to be customized on the destination server.

To track the history of promoted items on the destination server:

You can track the history of promoted workflows, steps, and functions using the history tab:

Promoted Item	How to Access	Description
Workflow	Automation > Workflows > <i><promoted_workflow></i> > History	Date: <i><date_time_of_promotion></i> Person: <i><user_that_promoted_workflow></i> Source: REST API Comment: Promoted using " <i><promote_workflow_that_imported_item></i> " from DMA server <i><server_name></i>
Step	Automation > Steps > <i><promoted_step></i> > History	Date: <i><date_time_of_promotion></i> Person: <i><user_that_promoted_step></i> Source: REST API Comment: Promoted with " <i><promoted_workflow></i> "
Function	Automation > Functions > <i><promoted_function></i> > History	Date: <i><date_time_of_promotion></i> Person: <i><user_that_promoted_function></i> Source: REST API Comment: Promoted with " <i><promoted_workflow></i> "

To use the promoted workflow on the destination server:

Before you run the newly promoted workflow, use the Preview report (file `promote_summary.txt`) to customize the following on the destination server:

- Password values
- Custom Field values

Set up the environment on the destination server:

- Environments: organizations, servers, instances, and databases
- Targets for deployments

Sample Scenarios

This topic shows you how to use various parameters to achieve the following workflow promotion scenarios in your environment when using **"Promote Workflow – Export and Import"**.

Scenario 1: Preview All Automation Items but Do Not Promote

In this scenario, all deployments, policies, and Smart Groups that are referenced by the workflow (or any of its deployments) are previewed but not promoted.

In this scenario, Preview Only is enabled by default.

In this scenario, Rollback on Error is enabled by default. The workflow and any related items that existed on the destination server prior to the promote operation will be restored in the event that the promote fails.

Example Parameter Values for Gather Parameters for Promote Workflow

Parameter Name	Example	Description								
Destination DMA Password	destpwd	Password for the user specified in the Destination DMA Username parameter.								
Destination DMA URL	see description	URL for the destination DMA server. For example: <code>https://dma2.mycompany.com:8443/dma</code>								
Destination DMA Username	admindest	DMA user who will perform the promote operation on the destination server.								
Export Location	/Oracle Workflows/workflow123.zip	The location where the exported DMA artifacts are stored. This can be either a fully qualified ZIP filename (default) or a fully qualified directory path—based on the advanced parameter Export Zip Archive. If it is a directory, a time-stamped sub-directory or ZIP file will be created to store the files. The location is on the target server.								
Roles on Destination Server	DMA Admins	<p>Comma-separated list of roles that will be assigned to promoted items. At least one role must be specified.</p> <p>All roles are assigned to the following promoted items (workflows, steps, deployments, and policies) that do not exist on the destination DMA server prior to the promote operation. The roles specified for these promoted items are given full permissions:</p> <table><tr><td>Workflow</td><td>READ, WRITE</td></tr><tr><td>Step</td><td>READ, WRITE</td></tr><tr><td>Deployment</td><td>READ, WRITE, EXECUTE</td></tr><tr><td>Policy</td><td>READ, WRITE</td></tr></table> <p>The first role specified in Roles on Destination Server is set in the Roles attribute for promoted Smart Groups that do not exist on the destination server prior to the promote operation.</p>	Workflow	READ, WRITE	Step	READ, WRITE	Deployment	READ, WRITE, EXECUTE	Policy	READ, WRITE
Workflow	READ, WRITE									
Step	READ, WRITE									
Deployment	READ, WRITE, EXECUTE									
Policy	READ, WRITE									

Example Parameter Values for Gather Parameters for Promote Workflow, continued

Parameter Name	Example	Description
		Role-based permissions for existing items are preserved. Note: If the roles do not yet exist on the destination server, you need to create them before attempting to promote.
Workflow Name	Run Oracle Compliance Check - CIS	Name of the workflow to be promoted.

Be sure that the default values for all remaining input parameters are appropriate for your environment (see ["Parameters for Promote Workflow - Export and Import" on page 1502](#)).

Scenario 2: Promote All Automation Items

In this scenario, all deployments, policies, and Smart Groups that are referenced by the workflow (or any of its deployments) are promoted.

In this scenario, Preview Only is set to NO.

The Database Compliance summary report will be emailed to a recipient.

In this scenario, Rollback on Error is enabled by default. The workflow and any related items that existed on the destination server prior to the promote operation will be restored in the event that the promote fails.

Example Parameter Values for Gather Parameters for Promote Workflow

Parameter Name	Example	Description								
Destination DMA Password	destpwd	Password for the user specified in the Destination DMA Username parameter.								
Destination DMA URL	see description	URL for the destination DMA server. For example: https://dma2.mycompany.com:8443/dma								
Destination DMA Username	admindest	DMA user who will perform the promote operation on the destination server.								
Export Location	/Oracle Workflows/workflow123.zip	The location where the exported DMA artifacts are stored. This can be either a fully qualified ZIP filename (default) or a fully qualified directory path—based on the advanced parameter Export Zip Archive. If it is a directory, a time-stamped sub-directory or ZIP file will be created to store the files. The location is on the target server.								
Preview Only	NO	If Preview Only is set to YES, the workflow will show you which items will be promoted, but it will not make any changes on the destination server. Valid values are YES/TRUE and NO/FALSE (case-insensitive).								
Roles on Destination Server	DMA Admins	<p>Comma-separated list of roles that will be assigned to promoted items. At least one role must be specified.</p> <p>All roles are assigned to the following promoted items (workflows, steps, deployments, and policies) that do not exist on the destination DMA server prior to the promote operation. The roles specified for these promoted items are given full permissions:</p> <table><tr><td>Workflow</td><td>READ, WRITE</td></tr><tr><td>Step</td><td>READ, WRITE</td></tr><tr><td>Deployment</td><td>READ, WRITE, EXECUTE</td></tr><tr><td>Policy</td><td>READ, WRITE</td></tr></table> <p>The first role specified in Roles on Destination Server is set in the Roles attribute for promoted Smart Groups that do not exist on the destination server prior to the promote operation.</p>	Workflow	READ, WRITE	Step	READ, WRITE	Deployment	READ, WRITE, EXECUTE	Policy	READ, WRITE
Workflow	READ, WRITE									
Step	READ, WRITE									
Deployment	READ, WRITE, EXECUTE									
Policy	READ, WRITE									

Example Parameter Values for Gather Parameters for Promote Workflow, continued

Parameter Name	Example	Description
		Role-based permissions for existing items are preserved. Note: If the roles do not yet exist on the destination server, you need to create them before attempting to promote.
Workflow Name	Run Oracle Compliance Check - CIS	Name of the workflow to be promoted.

The following parameter is not visible by default in a deployment. You need to expose it before you can use it.

Example Parameter Values for Gather Advanced Parameters for Promote Workflow - Import

Parameter Name	Example	Description
Email Address	JohnDoe@mycompany.com	Comma separated list of email addresses where the Database Compliance summary report will be sent.

Be sure that the default values for all remaining input parameters are appropriate for your environment (see ["Parameters for Promote Workflow - Export and Import" on page 1502](#)).

Scenario 3: Promote Only a Subset of Deployments, Policies, and Smart Groups

In this scenario, the deployments, policies, and Smart Groups to be promoted are specifically included or excluded.

- Included objects: Provided that these objects are referenced by the specified workflow or one (or more) of its deployments, the objects will be created or updated on the destination server. Any objects that are not explicitly specified will not be promoted.
- Excluded objects: All objects not in the exclude list that are referenced by the specified workflow or one (or more) of its deployments, the objects will be created or updated on the destination server.

In this scenario, Preview Only is set to NO.

In this scenario, Rollback on Error is enabled by default. The workflow and any related items that existed on the destination server prior to the promote operation will be restored in the event that the promote fails.

Example Parameter Values for Gather Parameters for Promote Workflow

Parameter Name	Example	Description
Destination DMA Password	destpwd	Password for the user specified in the Destination DMA Username parameter.
Destination DMA URL	see description	URL for the destination DMA server. For example: https://dma2.mycompany.com:8443/dma
Destination DMA Username	admindest	DMA user who will perform the promote operation on the destination server.
Export Location	/Oracle Workflows/workflow123.zip	The location where the exported DMA artifacts are stored. This can be either a fully qualified ZIP filename (default) or a fully qualified directory path—based on the advanced parameter Export Zip Archive. If it is a directory, a time-stamped sub-directory or ZIP file will be created to store the files. The location is on the target server.
Filter Deployments	INCLUDE: Run Oracle Compliance Check - CIS - Linux Svrs	A filter for deployments to be promoted. Valid values are ALL, NONE, INCLUDE: followed by a comma separated list of deployments to include, or EXCLUDE: followed by a comma separated list of deployments to exclude. The value ALL will promote all deployments associated with the workflow; the value NONE will not promote any of the deployments associated with the workflow. Note: Maximum number of characters is 1000.
Filter Policies	EXCLUDE: Oracle Test Compliance	A filter for policies to be promoted. Valid values are ALL, NONE, INCLUDE: followed by a comma separated list of policies to include, or EXCLUDE: followed by a comma separated list of policies to exclude. The value ALL will promote all policies

Example Parameter Values for Gather Parameters for Promote Workflow, continued

Parameter Name	Example	Description								
		<p>associated with the workflow; the value NONE will not promote any of the policies associated with the workflow.</p> <p>Note: Maximum number of characters is 1000.</p>								
Filter Smart Groups	INCLUDE: Linux Srvrs, Europe Srvrs	<p>A filter for Smart Groups to be promoted. Valid values are ALL, NONE, INCLUDE: followed by a comma separated list of Smart Groups to include, or EXCLUDE: followed by a comma separated list of Smart Groups to exclude. The value ALL will promote all Smart Groups associated with the workflow; the value NONE will not promote any of the Smart Groups associated with the workflow.</p> <p>Note: Maximum number of characters is 1000.</p>								
Preview Only	NO	<p>If Preview Only is set to YES, the workflow will show you which items will be promoted, but it will not make any changes on the destination server. Valid values are YES/TRUE and NO/FALSE (case-insensitive).</p>								
Roles on Destination Server	DMA Admins	<p>Comma-separated list of roles that will be assigned to promoted items. At least one role must be specified.</p> <p>All roles are assigned to the following promoted items (workflows, steps, deployments, and policies) that do not exist on the destination DMA server prior to the promote operation. The roles specified for these promoted items are given full permissions:</p> <table><tr><td>Workflow</td><td>READ, WRITE</td></tr><tr><td>Step</td><td>READ, WRITE</td></tr><tr><td>Deployment</td><td>READ, WRITE, EXECUTE</td></tr><tr><td>Policy</td><td>READ, WRITE</td></tr></table> <p>The first role specified in Roles on Destination Server is set in the Roles attribute for promoted Smart Groups that do not exist on the destination server prior to the promote operation.</p> <p>Role-based permissions for existing items are preserved.</p> <p>Note: If the roles do not yet exist on the destination server, you need to create them before attempting to promote.</p>	Workflow	READ, WRITE	Step	READ, WRITE	Deployment	READ, WRITE, EXECUTE	Policy	READ, WRITE
Workflow	READ, WRITE									
Step	READ, WRITE									
Deployment	READ, WRITE, EXECUTE									
Policy	READ, WRITE									
Workflow Name	Run Oracle Compliance Check - CIS	<p>Name of the workflow to be promoted.</p>								

Be sure that the default values for all remaining input parameters are appropriate for your environment.

Parameters for Promote Workflow - Export and Import

The following tables describe the required and optional input parameters for this workflow. For some parameters, if you do not specify a value for a parameter, a default value is assigned.

Input Parameters Defined in this Step: Gather Parameters for Promote Workflow

Parameter Name	Default Value	Required	Description
Destination DMA Password	no default	required	Password for the user specified in the Destination DMA Username parameter.
Destination DMA URL	no default	required	URL for the destination DMA server. For example: <code>https://dma2.mycompany.com:8443/dma</code>
Destination DMA Username	no default	required	DMA user who will perform the promote operation on the destination server.
Export Location	no default	required	The location where the exported DMA artifacts are stored. This can be either a fully qualified ZIP filename (default) or a fully qualified directory path—based on the advanced parameter Export Zip Archive. If it is a directory, a time-stamped sub-directory or ZIP file will be created to store the files. The location is on the target server.
Filter Deployments	ALL	required	A filter for deployments to be promoted. Valid values are ALL, NONE, INCLUDE: followed by a comma separated list of deployments to include, or EXCLUDE: followed by a comma separated list of deployments to exclude. The value ALL will promote all deployments associated with the workflow; the value NONE will not promote any of the deployments associated with the workflow. Note: Maximum number of characters is 1000.
Filter Policies	ALL	required	A filter for policies to be promoted. Valid values are ALL, NONE, INCLUDE: followed by a comma separated list of policies to include, or EXCLUDE: followed by a comma separated list of policies to exclude. The value ALL will promote all policies associated with the workflow; the value NONE will not promote any of the policies associated with the workflow. Note: Maximum number of characters is 1000.
Preview Only	YES	required	If Preview Only is set to YES, the workflow will show you which items will be promoted, but it will not make any changes on the destination server. Valid values are YES/TRUE and NO/FALSE (case-insensitive).
Filter Smart Groups	ALL	required	A filter for Smart Groups to be promoted. Valid values are ALL, NONE, INCLUDE: followed by a comma separated list of Smart Groups to include, or EXCLUDE: followed by a comma separated list of Smart Groups to exclude. The value ALL will promote all Smart Groups associated with the workflow; the

Input Parameters Defined in this Step: Gather Parameters for Promote Workflow , continued

Parameter Name	Default Value	Required	Description								
			<p>value NONE will not promote any of the Smart Groups associated with the workflow.</p> <p>Note: Maximum number of characters is 1000.</p>								
Roles on Destination Server	no default	required	<p>Comma-separated list of roles that will be assigned to promoted items. At least one role must be specified.</p> <p>All roles are assigned to the following promoted items (workflows, steps, deployments, and policies) that do not exist on the destination DMA server prior to the promote operation. The roles specified for these promoted items are given full permissions:</p> <table><tr><td>Workflow</td><td>READ, WRITE</td></tr><tr><td>Step</td><td>READ, WRITE</td></tr><tr><td>Deployment</td><td>READ, WRITE, EXECUTE</td></tr><tr><td>Policy</td><td>READ, WRITE</td></tr></table> <p>The first role specified in Roles on Destination Server is set in the Roles attribute for promoted Smart Groups that do not exist on the destination server prior to the promote operation.</p> <p>Role-based permissions for existing items are preserved.</p> <p>Note: If the roles do not yet exist on the destination server, you need to create them before attempting to promote.</p>	Workflow	READ, WRITE	Step	READ, WRITE	Deployment	READ, WRITE, EXECUTE	Policy	READ, WRITE
Workflow	READ, WRITE										
Step	READ, WRITE										
Deployment	READ, WRITE, EXECUTE										
Policy	READ, WRITE										
Workflow Name	no default	required	Name of the workflow to be promoted.								

The following parameters are not visible by default in a deployment. You need to expose them before you can use them.

Additional Input Parameters Defined in this Step: Gather Advanced Parameters for Promote Workflow

Parameter Name	Default Value	Required	Description
Email Address	no default	optional	Comma separated list of email addresses where the Database Compliance summary report will be sent.
Export Zip Archive	YES	optional	<p>Flag to indicate whether the workflow (and related automation items) and log files are exported as a ZIP file.</p> <p>If set to YES or TRUE (the default), the files are exported to a ZIP file.</p> <p>If set to NO or FALSE, the files are exported to a time-stamped sub-directory of the Export Location.</p>
Ignore Platform Version	NO	optional	<p>If set to NO (default), the Database Compliance workflows check that the source and destination DMA platform versions are the same. If set to YES, the Database Compliance workflows ignore different DMA platform versions and will attempt to promote the workflow anyway. Valid values are YES/TRUE and NO/FALSE (case-insensitive).</p> <p>Caution: Promote does not officially support promoting between different versions. Use at your own risk.</p>
Rollback on Error	YES	optional	Set to NO if you do NOT want DMA to rollback the workflow and all related items on the destination server to their original state in the event that the promote operation fails. Valid values are YES/TRUE and NO/FALSE (case-insensitive).

Discovery

DMA provides special Discovery workflows that you can use to automatically discover instances, databases, and middleware residing on your managed servers. You can run the Discovery workflows manually, or you can set up scheduled deployments to run them periodically. This workflow discovers as much about a physical environment's SQL Server, Oracle, Sybase, and DB2 databases. This workflow also discovers WebSphere, JBoss, and WebLogic application server products. Instances that are "up" will provide more information than instances that are "down".

The Discovery workflow is only additive. It will not remove instances or databases currently in your environment.

Note: In cluster situations where one node is active while other nodes are inactive, Discovery will only find instances and databases on the active node. Nothing will be added to inactive nodes.

The workflow performs validation checks at the operating system level, including file system space checks.

Topic	Information Included
"How this Workflow Works" on page 1508	Information about what the workflow does, including validation checks performed, steps executed, and a high-level process flow
"How to Run this Workflow" on page 1510	Instructions for running this workflow in your environment
"Sample Scenarios" on page 1512	Examples of typical parameter values for this workflow
"Parameters for Discovery" on page 1513	List of input parameters for this workflow

The process of deploying and running this workflow is the same for all scenarios, but the parameters required will differ depending on the specific scenario that you are implementing.

The workflow provides default values for most parameters. These default values are usually sufficient for a typical provisioning scenario. You can override the defaults by specifying parameter values in the deployment. You can also expose additional parameters in the workflow, if necessary, to accomplish more advanced scenarios.

Any parameters not explicitly specified in the deployment will have the default values listed in ["Parameters for Discovery" on page 1513](#).

Note: The documentation for this workflow contains steps that are referred to by their base names. The names in the DMA user interface may have a version appended, for example, v2.

Prerequisites for this Workflow

The following prerequisites must be satisfied before you can run the Apache - Provision Software workflow:

1. The workflow requires unchallenged `sudo` access to a user (typically root) who can access all required files and directories.
2. The workflow requires OpenSSL to be installed.
3. Adequate disk space must be available to install the Apache web server binaries.
4. This workflow deploys the Apache distribution archive file. You must compile and build the Apache archive file before running this workflow.

For information about prerequisites for Apache Tomcat, refer to the [Apache HTTP Server Documentation](#).

How this Workflow Works

This topic contains the following information about the Discovery workflow:

Steps Executed

The Discovery workflow includes the following steps. Each step must complete successfully before the next step can start. If a step fails, the workflow reports a failure, and subsequent steps are skipped.

Process Flow

This workflow performs the following tasks:

1. Gathers mandatory and optional input parameters (user-provided) to run Discovery workflow.
2. Validates if Oracle discovery is enabled.
3. If true, audits the server's physical environment looking for Oracle instances and databases.

In cluster situations where one node is active while other nodes are inactive, Discovery will only find instances and databases on the active node.

4. Validates if SQL Server discovery is enabled.
5. Audits the server's physical environment looking for SQLServer instances and databases.
6. Validates if DB2 discovery is enabled.
7. Audits the server's physical environment looking for DB2 databases.
8. Validates if Oracle discovery is enabled.
9. Audits the server's physical environment looking for Oracle instances and databases.
10. Validates if MySQL discovery is enabled.
11. Discovers the MySQL instances and databases on the target machine.
12. Validates if WebSphere discovery is enabled.
13. Audits the server's physical environment looking for WebSphere cells, clusters, and managed servers.
14. Validates if WebLogic discovery is enabled.
15. Audits the server's physical environment looking for WebLogic domains, clusters, and managed servers.
16. Validates if JBoss discovery is enabled.
17. Audits the server's physical environment looking for JBoss instances.
18. Validates if Apache Tomcat discovery is enabled.
19. Audits the server's physical environment looking for Apache Tomcat instances.
20. Validates if Apache Tomcat web server discovery is enabled.
21. Audits the server's physical environment looking for Apache Tomcat web server instances.
22. Gathers summary of discovery of databases and application servers.

How to Run this Workflow

This topic explains how to customize and run the Discovery workflow in your environment.

To customize and run the Apache - Provision Software workflow:

1. Create a deployable copy of the workflow.
2. Determine the values that you will specify for the following parameters. These are the parameters that are visible in the deployment by default.

Parameters in the step: Gather Parameters for Discovery

Parameter Name	Default Value	Description
Run Apache Tomcat Server Middleware	True	If value is True, then the Apache Tomcat Server middleware platform will be discovered and updated in DMA. If value is False, the Apache Tomcat Server middleware platform will not be discovered and updated in DMA.
Run Apache Web Server Middleware	True	If value is True, then the Apache web server middleware platform will be discovered and updated in DMA. If value is False, the Apache web server middleware platform will not be discovered and updated in DMA.
Run DB2 Database	True	If value is True, then the DB2 database platform will be discovered and updated in DMA. If value is False, the DB2 database platform will not be discovered and updated in DMA.
Run JBoss Middleware	True	If value is True, then the JBoss middleware platform will be discovered and updated in DMA. If value is False, the JBoss middleware platform will not be discovered and updated in DMA.
Run MySQL Database	True	If value is True, then the MySQL server database platform will be discovered and updated in DMA. If value is False, the MySQL server database platform will not be discovered and updated in DMA.
Run Oracle Database	True	If value is True, then the Oracle database platform will be discovered and updated in DMA. If value is False, the Oracle database platform will not be discovered and updated in DMA.
Run SQL Server Database	True	If value is True, then the SQL server database platform will be discovered and updated in DMA. If value is False, the SQL server database platform will not be discovered and updated in DMA.
Run Sybase Database	True	If value is True, then the Sybase database platform will be discovered and updated in DMA. If value is False, the Sybase database platform will not be discovered and updated in DMA.
Run WebSphere Middleware	True	If value is True, then the Weblogic middleware platform will be discovered and updated in DMA. If value is False, the Weblogic middleware platform will not be discovered and updated in DMA.
Run Weblogic Middleware	True	If value is True, then the WebSphere middleware platform will be discovered and updated in DMA. If value is False, the WebSphere middleware platform will not be discovered and updated in DMA.

See ["Parameters for Discovery" on page 1513](#) for detailed descriptions of all input parameters for this workflow, including default values.

3. In the workflow editor, expose any additional parameters that you need. You will specify values for those parameters when you create the deployment.
4. Save the changes to the workflow (click **Save** in the lower right corner).
5. Create a new deployment.
6. On the Parameters tab, specify values for the required parameters listed in step 2 and any additional parameters that you have exposed. You do not need to specify values for those parameters whose default values are appropriate for your environment.
7. On the Targets tab, specify one or more targets for this deployment.
8. Save the changes to the workflow (click **Save** in the lower right corner).
9. Run the workflow using this deployment.

The workflow will complete and report "Success" on the Console if it has run successfully. If an invalid parameter value is specified, an error is logged, and the workflow terminates in the "Failure" state.

Sample Scenarios

This topic shows you how to use various parameters to achieve the following provisioning scenarios in your environment using the Discovery workflow.

Step Name	Parameter Name	Example Value
Gather Parameters for Discovery	Run Apache Tomcat Server Middleware	True
	Run Apache Web Server Middleware	True
	Run DB2 Database	True
	Run JBoss Middleware	True
	Run MySQL Database	True
	Run Oracle Database	True
	Run SQL Server Database	True
	Run Sybase Database	True
	Run WebSphere Middleware	True
	Run Weblogic Middleware	True

Be sure that the default values for all remaining parameters are appropriate for your environment.

Parameters for Discovery

The following table describes the required input parameters for this workflow. Several of these parameters are not initially visible in a deployment. For many parameters, if you do not specify a value for a parameter, a default value is assigned.

Parameters in the step: Gather Parameters for Discovery

Parameter Name	Default Value	Description
Run Apache Tomcat Server Middleware	True	If value is True, then the Apache Tomcat Server middleware platform will be discovered and updated in DMA. If value is False, the Apache Tomcat Server middleware platform will not be discovered and updated in DMA.
Run Apache Web Server Middleware	True	If value is True, then the Apache web server middleware platform will be discovered and updated in DMA. If value is False, the Apache web server middleware platform will not be discovered and updated in DMA.
Run DB2 Database	True	If value is True, then the DB2 database platform will be discovered and updated in DMA. If value is False, the DB2 database platform will not be discovered and updated in DMA.
Run JBoss Middleware	True	If value is True, then the JBoss middleware platform will be discovered and updated in DMA. If value is False, the JBoss middleware platform will not be discovered and updated in DMA.
Run MySQL Database	True	If value is True, then the MySQL server database platform will be discovered and updated in DMA. If value is False, the MySQL server database platform will not be discovered and updated in DMA.
Run Oracle Database	True	If value is True, then the Oracle database platform will be discovered and updated in DMA. If value is False, the Oracle database platform will not be discovered and updated in DMA.
Run SQL Server Database	True	If value is True, then the SQL server database platform will be discovered and updated in DMA. If value is False, the SQL server database platform will not be discovered and updated in DMA.
Run Sybase Database	True	If value is True, then the Sybase database platform will be discovered and updated in DMA. If value is False, the Sybase database platform will not be discovered and updated in DMA.
Run WebSphere Middleware	True	If value is True, then the Weblogic middleware platform will be discovered and updated in DMA. If value is False, the Weblogic middleware platform will not be discovered and updated in DMA.
Run Weblogic Middleware	True	If value is True, then the WebSphere middleware platform will be discovered and updated in DMA. If value is False, the WebSphere middleware platform will not be discovered and updated in DMA.

Send documentation feedback

If you have comments about this document, you can [contact the documentation team](#) by email. If an email client is configured on this system, click the link above and an email window opens with the following information in the subject line:

Feedback on User Guide (Database and Middleware Automation 10.50.001.000)

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to hpe_dma_docs@hpe.com.

We appreciate your feedback!