HP Database and Middleware Automation

For Linux, Solaris, AIX, and Windows®

Software Version: 10.10

WebSphere Configuration Management

User Guide

Document Release Date: June 2013

Software Release Date: June 2013

Legal Notices

Warranty

The only warranties for HP 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. HP 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 HP 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

© Copyright 2013 Hewlett-Packard Development Company, L.P.

Trademark Notices

Oracle® and Java® are registered trademarks of Oracle and/or its affiliates.

UNIX® is a registered trademark of The Open Group.

Windows® is a U.S. registered trademark of Microsoft Corporation.

Documentation Updates

The title page of this document contains the following identifying information:

- Software Version number, which indicates the software version.
- Document Release Date, which changes each time the document is updated.
- Software Release Date, which indicates the release date of this version of the software.

To check for recent updates or to verify that you are using the most recent edition of a document:

http://h20230.www2.hp.com/selfsolve/manuals

This site requires that you register for an HP Passport and sign in. To register for an HP Passport ID, go to:

http://h20229.www2.hp.com/passport-registration.html

Or click the **New users - please register** link 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 HP sales representative for details.

The following table indicates changes made to this document since the last released edition.

Document Changes

Chapter	Version	Changes
Title Page Legal Notices	10.10	Updated version number, software release date, document release date, and copyright date range.
About HP DMA Solution Packs	10.10	Added overview topic: About HP DMA Solution Packs.

Support

Visit the HP Software Support Online web site at:

http://www.hp.com/go/hpsoftwaresupport

This web site provides contact information and details about the products, services, and support that HP Software offers.

HP Software online support provides customer self-solve capabilities. It provides a fast and efficient way to access interactive technical support tools needed to manage your business. As a valued support customer, you can benefit by using the support web site to:

- Search for knowledge documents of interest
- Submit and track support cases and enhancement requests
- Download software patches
- Manage support contracts
- Look up HP support contacts
- Review information about available services
- Enter into discussions with other software customers
- Research and register for software training

Most of the support areas require that you register as an HP Passport user and sign in. Many also require a support contract. To register for an HP Passport ID, go to:

http://h20229.www2.hp.com/passport-registration.html

To find more information about access levels, go to:

http://h20230.www2.hp.com/new_access_levels.jsp

Contents

Contents 5

About HP DMA Solution Packs 7

Audience 8

Document Map 9

Important Terms 10

The WebSphere Configuration Management Solution 11

What this Solution Includes 12

Supported Products and Platforms 13

Prerequisites 14

WebSphere Configuration Management Quick Start 15

Import the Solution Pack 16

Create a Deployable Workflow 19

Create a Deployment 20

Run Your Workflow 22

View the Results 23

Workflow Details 25

Configure WebSphere Cluster and Cluster Members 27

Prerequisites for this Workflow 29

How this Workflow Works 30

How to Run this Workflow 34

Sample Scenario 37

Parameters for Configure WebSphere Cluster and Cluster Members 45

Create and Configure WebSphere Data Sources 47

Prerequisites for this Workflow 49

How this Workflow Works 50

How to Run this Workflow 55

Sample Scenario 59

Parameters for Create and Configure WebSphere Data Sources 67
Create and Configure WebSphere Web Server Definitions 70
Prerequisites for this Workflow 71
How this Workflow Works 72
How to Run this Workflow 76
Sample Scenario 79
Parameters for Create and Configure WebSphere Web Server Definitions 83
Reference Information 85
WebSphere Product Documentation 85
Database Product Documentation 85
Oracle Database Product Documentation 86
Microsoft SQL Server Documentation 86
HP DMA Documentation 86
Tips and Best Practices 87
How a Solution Pack is Organized 88
How to Expose Additional Workflow Parameters 92
How to Use a Policy to Specify Parameter Values 93
Create a Policy 93
Extract a Policy 94
Reference the Policy in the Deployment 94
How to Import a File into the Software Repository 96
Troubleshooting 97
Target Type 97
User Permissions and Related Requirements 97
Discovery in HP DMA 98
Glossary 99

About HP DMA Solution Packs

HP Database and Middleware Automation (HP DMA) software automates administrative tasks like provisioning and configuration, compliance, patching, and release management for databases and application servers. When performed manually, these day-to-day operations are error-prone, time consuming, and difficult to scale.

HP DMA automates these daily, mundane, and repetitive administration tasks that take up 60-70% of a database or application server administrator's day. Automating these tasks enables greater efficiency and faster change delivery with higher quality and better predictability.

HP DMA provides role-based access to automation content. This enables you to better utilize resources at every level:

- End-users can deliver routine, yet complex, DBA and middleware tasks.
- Operators can execute expert level tasks across multiple servers including provisioning, patching, configuration, and compliance checking.
- Subject matter experts can define, enforce, and audit full stack automation across network, storage, server, database, & middleware.

An HP DMA workflow performs a specific automated task—such as provisioning database or application servers, patching database or application servers, or checking a database or application server for compliance with a specific standard. You specify environment-specific information that the workflow requires by configuring its parameters.

Related HP DMA workflows are grouped together in solution packs. When you purchase or upgrade HP DMA content, you are granted access to download specific solution packs.

Audience

This solution is designed for:

- IT architects and engineers who are responsible for planning, implementing, and maintaining application server environments using IBM WebSphere Application Server Network Deployment (WebSphere).
- Engineers who are implementing—or planning to implement—HP Database and Middleware Automation (HP DMA)

To use this solution, you should be familiar with WebSphere and its requirements (see links to the WebSphere Product Documentation on page 85).

Document Map

The following table shows you how to navigate this guide:

Topic	Description
The WebSphere Configuration Management Solution	General information about this solution, including what it contains and what it does.
WebSphere Configuration Management Quick Start	A step-by-step tutorial that shows you how to run the workflows.
Workflow Details	Information about the WebSphere workflows included in this solution, including: prerequisites, how it works, how to run it, sample scenarios, and a list of input parameters.
Reference Information	Links to current WebSphere product documentation and additional HP DMA documentation.
Tips and Best Practices	Simple procedures that you can use to accomplish a variety of common HP DMA tasks.
Troubleshooting	Tips for solving common problems.

Important Terms

Here are a few basic HP DMA terms that you will need to know:

- In HP DMA, a **workflow** executes a process —such as installing a software product or checking a database instance for compliance with a specific security benchmark.
- A workflow consist of a sequence of **steps**. Each step performs a very specific task. Steps can be shared among workflows.
- Steps can have input and output **parameters**, whose values will be unique to your environment.

  If you provide correct values for the input parameters that each scenario requires, the workflow will be able to accomplish its objective.Output parameters from one step often serve as input parameters to another step.
- A **solution pack** contains a collection of related workflows and the steps, functions, and policies that implement each workflow.

  More precisely, solution packs contain **workflow templates**. These are read-only versions of the workflows that cannot be deployed. To run a workflow included in a solution pack, you must first create a deployable copy of the workflow template and then customize that copy for your environment.
- The umbrella term **automation items** is used to refer to those items to which role-based permissions can be assigned. Automation items include workflows, deployments, steps, and policies.

  Organizations also have role-based permissions. Servers, instances, and databases inherit their role-based permissions from the organization in which the server resides.
- The **software repository** contains any files that a workflow might need to carry out its purpose (for example, software binaries or patch archives). If the files that a workflow requires are not in the software repository, they must be stored locally on each target server.

  When you are using HP DMA with HP Server Automation (HP SA), the software repository is the HP SA Software Library.
- An **organization** is a logical grouping of servers. You can use organizations to separate development, staging, and production resources—or to separate logical business units. Because user security for running workflows is defined at the organization level, organizations should be composed with user security in mind.

Additional terms are defined in the Glossary on page 99.

Chapter 1

The WebSphere Configuration Management Solution

The WebSphere configuration management solution provides tools that you can use to manage the configuration of your WebSphere Application Server. It makes your provisioned WebSphere system useable.

These tools enable you to:

WebSphere Feature	Functionality
WebSphere clusters and cluster members	• Create WebSphere clusters • Add cluster members to the newly-created cluster • Create initial and maximum heap sizes for the newly-created cluster member • Create logging attributes based on time, size, and location for each cluster member
WebSphere data sources	• Create data sources for Oracle or SQL Server databases • Customize the Java Database Connectivity (JDBC) provider • Customize the Java 2 Connector (J2C) alias • Configure the Java Name Directory Interface (JNDI) name • Configure minimum and maximum pool connections
WebSphere web server definitions	• Create an unmanaged node where web servers can run • Define a web server under the unmanaged node

By consistently using the tools provided in this solution, you can quickly, efficiently, and accurately configure your WebSphere Application Server environment. You maintain flexibility over the WebSphere environment by configuring environment-specific information through the input parameters.

What this Solution Includes

The Application Server Configuration Management solution pack contains the following WebSphere configuration management workflows:

Workflow Name	Purpose
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.
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.
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.

Supported Products and Platforms

The WebSphere configuration management workflows are supported on Red Hat Enterprise Linux, Solaris, and Windows platforms.

Product Platform

This solution pack is available for WebSphere 7 or WebSphere 8.

Operating Systems

For specific target operating system versions supported by each workflow, see the *HP Database and Middleware Automation Support Matrix* available on the HP Software Product Manuals web site:

http://h20230.www2.hp.com/selfsolve/manuals

Hardware Requirements

For HP DMA server hardware requirements, see the *HP DMA Installation Guide* and the *HP DMA Release Notes*.

HP Software Requirements

This solution requires HP DMA version 10.10 (or later).

Prerequisites

The following prerequisites must be satisfied before you can run the WebSphere configuration management workflows in this solution pack:

- You must have a working WebSphere Network Deployment cell version 7 or 8, with the Deployment Manager available for communication.
- You must run the Discover WebSphere workflow before you run the configuration management 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 HP DMA environment.

Note: Be sure to review the additional prerequisites for each workflow.

Chapter 2

WebSphere Configuration Management Quick Start

This tutorial shows you how to run one of the workflows, Configure WebSphere Cluster and Cluster Members, in the Application Server Configuration Management Solution Pack. You can use this tutorial as an example for running the other configuration management workflows.

The tutorial will guide you through the following basic steps to import the Application Server Configuration Management Solution Pack and then to run the workflow:

1. Import the Solution Pack on the next page
2. Create a Deployable Workflow on page 19
3. Create a Deployment on page 20
4. Run Your Workflow on page 22
5. View the Results on page 23

You can follow the same steps to run the other configuration management workflows.

In this tutorial, default values will be used for most input parameters. Before executing these steps, make sure that these default values are suitable for your environment.

Note: See the "Parameter" topic associated with each workflow for descriptions of all available input parameters for your workflow, including default values.

The information presented in this tutorial assumes the following:

- HP DMA is installed and operational.
- At least one valid target is available.

Note: This tutorial is included in every HP DMA solution pack user guide. To skip directly to information about the Application Server Configuration Management workflows, see the Workflow Details.

Import the Solution Pack

The following instructions assume that you have purchased a license for the HP DMA solution pack that you want to import.

The HP DMA 10.10 solution packs are included on the HP DMA 10.10 installation media. They are located in the following folders:

- The `DMA_10.10_Server_and_Client` folder contains the Discovery solution pack.

  The Discovery solution pack is not automatically installed with HP DMA. You must import it if you want to use the discovery workflows.

- The `DMA_10.10_Database_Solution_Packs` folder contains all of the database solution packs (provisioning, advanced provisioning, patching, advanced patching, compliance, refresh, and release management).

- The `DMA_10.10_Middleware_Solution_Packs` folder contains all of the application server solution packs (provisioning, patching, configuration management, and release management).

Note: Always check to see if there are more recent versions of the HP DMA solution packs available online. Due to frequent releases, it is likely that the solution packs provided on the installation media have since been updated.

To get the most recent version of a solution pack:

1. Go to the following web site: HP Software Support Online
2. Go to the Self-Solve tab, and sign in using your HP Passport credentials (see Support on page 4 for more information).
3. On the Advanced Search page, specify the following search criteria:

Product:	Database and Middleware Automation
Version:	All Versions
Operating System:	All Operating Systems
Document Type:	Patches

4. Click **Search**.
5. If there is a more recent version of the Application Server Configuration Management solution pack that you want to import, do the following:
   a. Click the link for the solution pack that you want to import (for example: AS ConfMgt 10.x).
   b. Click the **DOWNLOAD PATCH** link, and download the ZIP file that contains the patch.
   c. From the patch ZIP file, extract the ZIP file that contains the solution pack (for example: ASConfigManagement.zip).

      Note: This ZIP file may be included in a larger ZIP file that contains multiple solution packs.

To import the solution pack:

1. On the system where you downloaded the solution pack, open a web browser, and go to the following address:

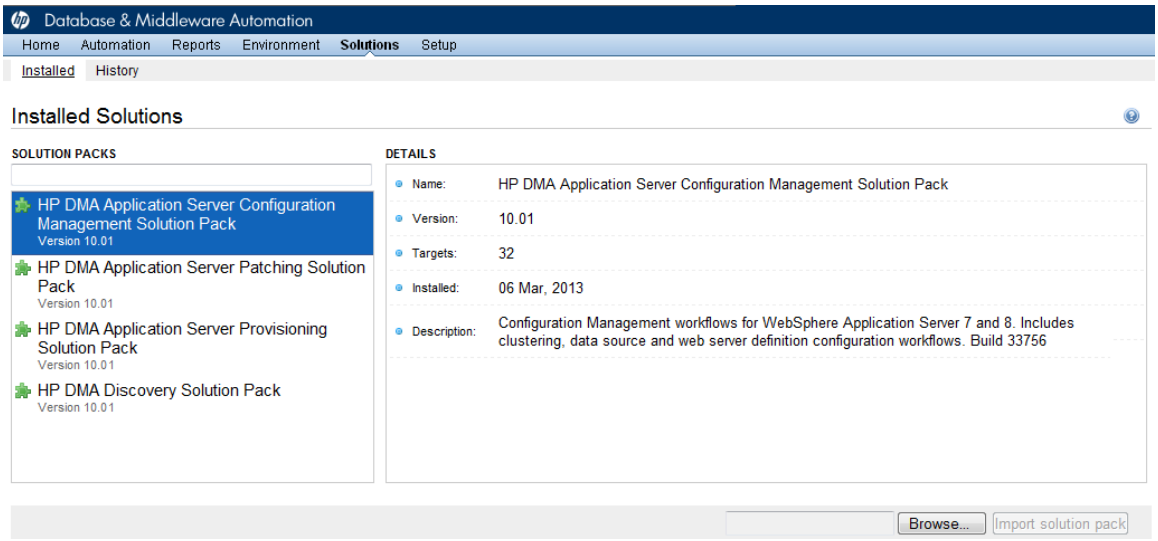
   `https://<HP_DMAserver>:8443/dma/login`

2. Log in to the HP DMA server using an account with Administrator capability.
3. On the Solutions > Installed tab, click the **Browse** button in the lower right corner. The Choose File dialog opens.

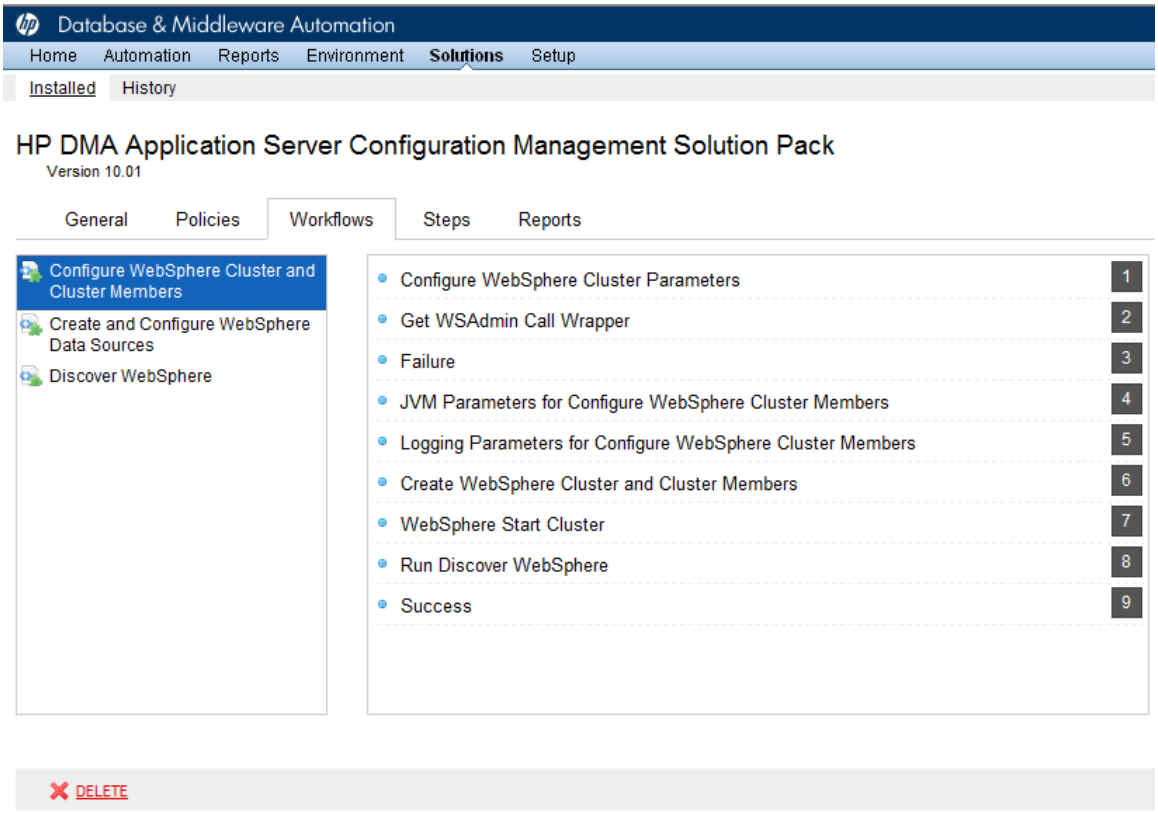
   Note: This button and the dialog that subsequently opens may have different names depending on the browser that you are using.

4. Locate and select the solution pack ZIP file that you extracted earlier, and click **Open**.
5. Click **Import solution pack**.

To view basic information about the solution pack, hover your mouse over its name in the left pane:



To view detailed information about the solution pack, click its name in the left pane. To view a list of the workflows that the solution pack contains, go to the Workflows tab.



Create a Deployable Workflow

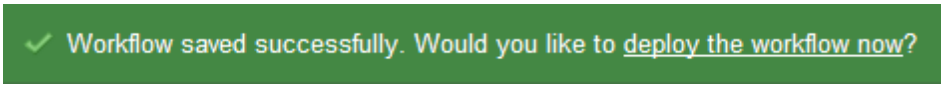
The workflow templates provided by HP in your solution pack are read-only and cannot be deployed. When you are viewing a read-only item in the HP DMA web UI, you will see the lock icon in the lower right corner:

Read-only workflows are not deployable. You can create a deployable workflow by making a copy of a workflow template.[1]

To create a deployable copy of the workflow template:

1. In the HP DMA web interface, go to Solutions > Installed.
2. In the left pane, click the Application Server Configuration Management Solution Pack.
3. Go to the Workflows tab.
4. From the list of workflows, select the Configure WebSphere Cluster and Cluster Members template.
5. Click the **Copy** button in the lower left corner.
6. On the Documentation tab, specify the following:
   - Name – Name that will appear in the list of available workflows
   - Tags – Keywords that you can use later to search for this workflow (optional)
   - Type – OS (this will be selected as a result of the copy)
   - Target level – Instance (this will be selected as a result of the copy)
7. On the Roles tab, grant Read access to at least one user or group and Write access to at least one user or group.
8. Click **Save**.

   Your new workflow now appears in the list of available workflows, and the following message is displayed:

9. Click the **deploy the workflow now** link in the green message bar.

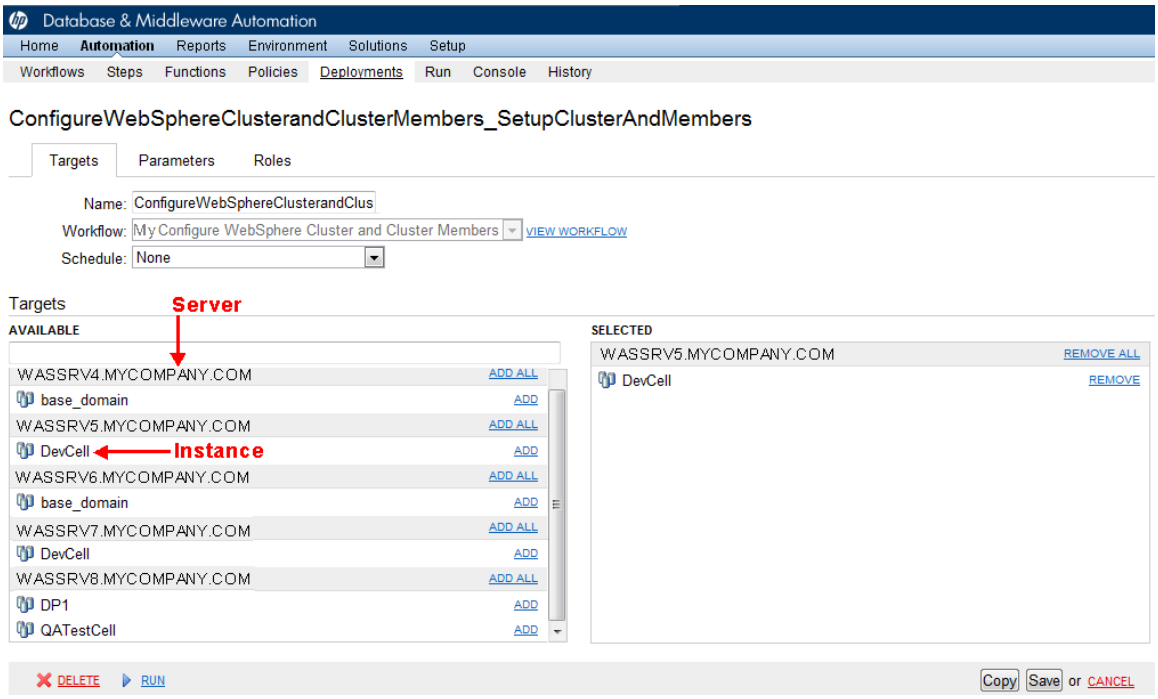
[1] For more information about creating and working with workflows, see "Workflows" in the *HP DMA User Guide*. This document is available on the HP Software Product Manuals web site: http://h20230.www2.hp.com/selfsolve/manuals

Create a Deployment

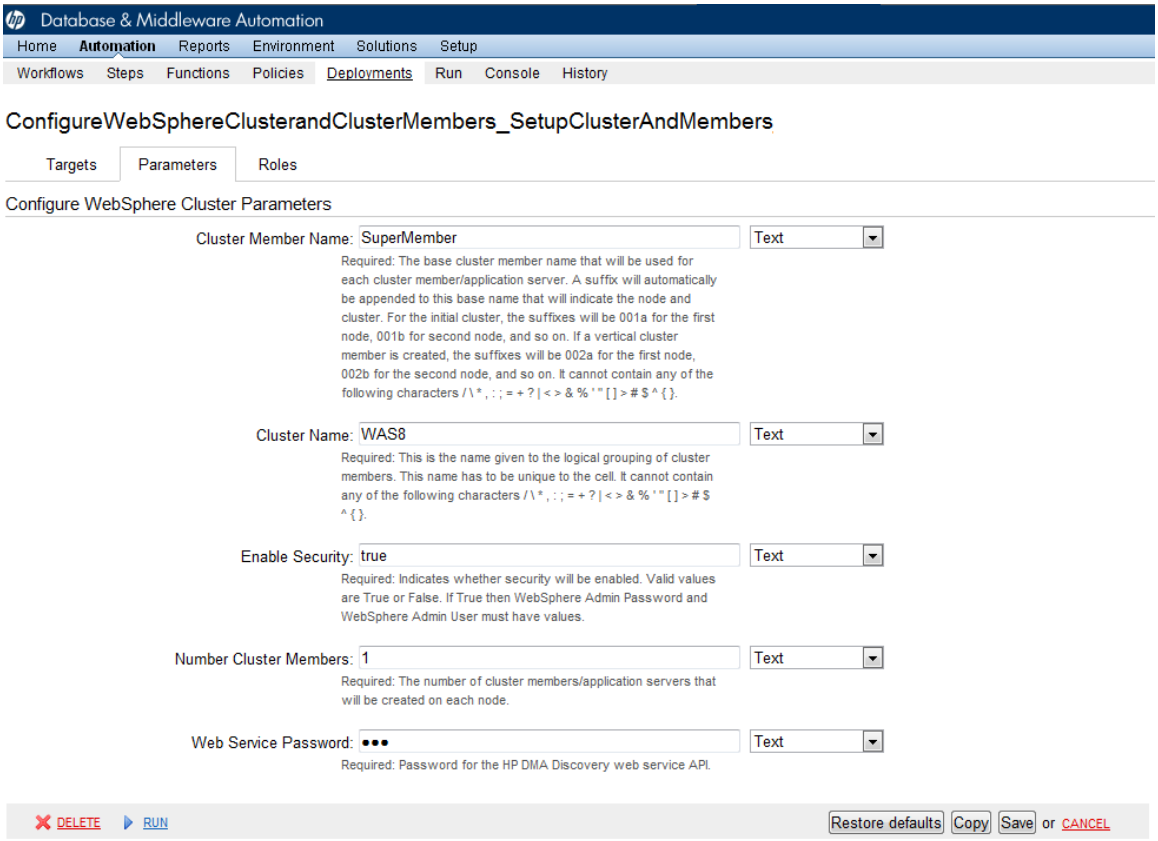
Before you can run your new workflow, you must create a deployment. A deployment associates a workflow with one or more specific targets (servers, instances, or databases).

To create a deployment:

1. If you do not see the green message bar—for example, if you navigated to another page after you created your copy of the workflow template—follow these steps:
   a. Go to the Automation > Deployments page.
   b. In the lower right corner, click **New deployment**.
2. Specify the following:
   - Name – Name that will appear in the list of available deployments.
   - Workflow – From the drop-down list, select the deployable workflow (the copy) that you just created.
   - Schedule – Frequency or date when the workflow will run. Select None so that the workflow will run once when you explicitly tell it to run.
3. From the list of AVAILABLE targets on the left side of the Targets area, click the **ADD** link for the instance where the workflow will run.



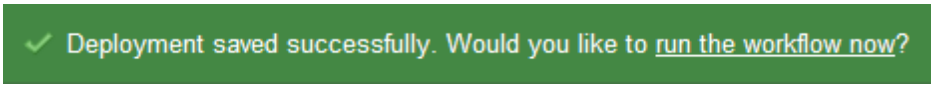
4. On the Parameters tab, specify values for the following input parameters:



Note: These are a subset of the required parameters for this workflow. Parameters that are not visible in the deployment will have default values. See Parameters for Configure WebSphere Cluster and Cluster Members on page 45 for descriptions of all available input parameters for this workflow, including default values.

5. Click **Save**.

   Your new deployment now appears in the list of available workflows, and the following message is displayed:



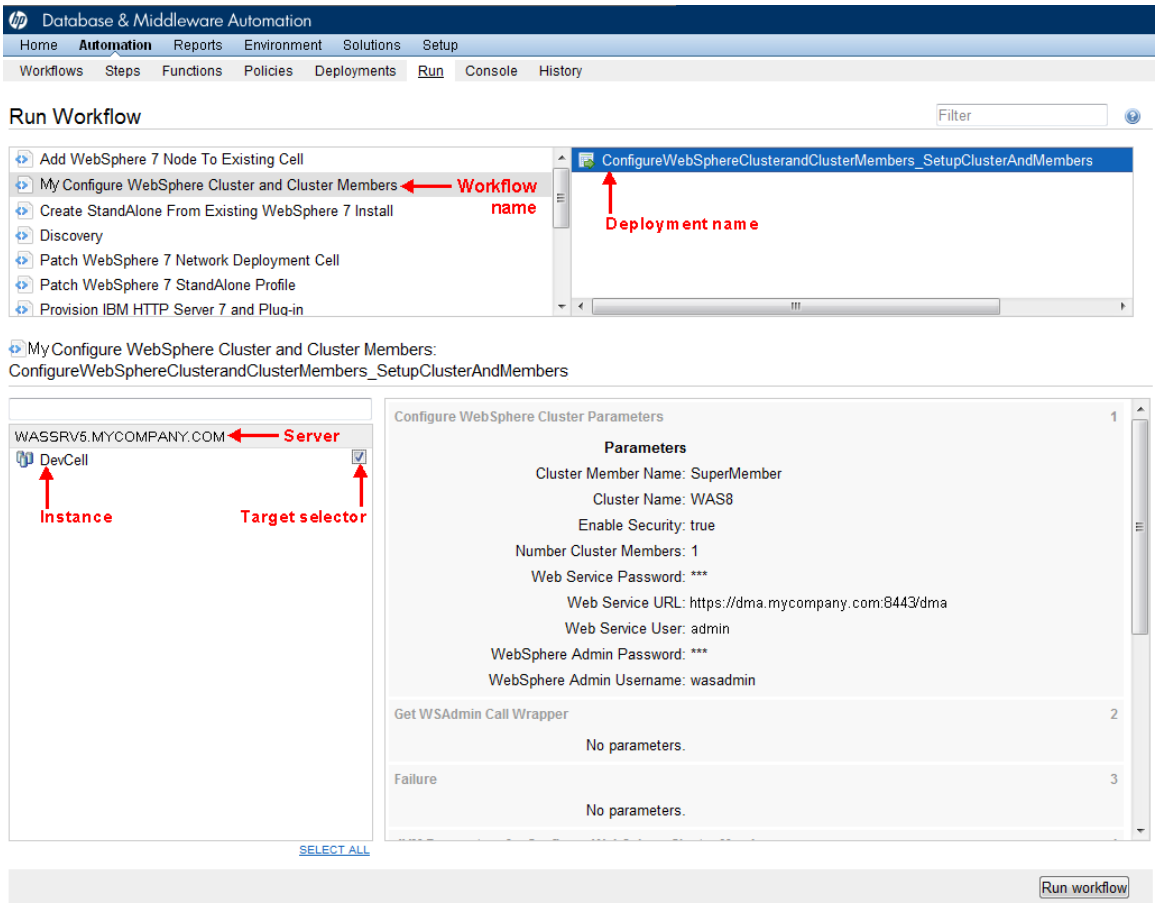
6. Click the **run the workflow now** link in the green message bar.

Run Your Workflow

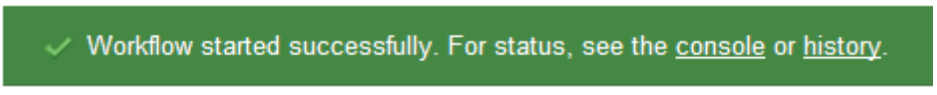
Now you are ready to run your workflow against the target that you selected.

To run the workflow:

1. If you do not see the green message bar—for example, if you navigated to another page after you created your deployment—follow these steps: show
   a. Go to the Automation > Run area.
   b. In the list of WORKFLOWS on the left side, select the workflow that you created.
   c. In the list of DEPLOYMENTS on the right side, select the deployment that you just created.
2. Select the target selector check box for the instance where you want to run the workflow.



3. Click the **Run workflow** button.
4. The following message is displayed:

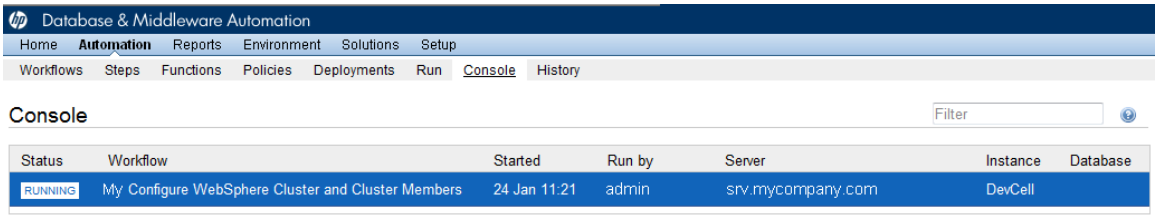


5. To view the progress of your deployment, click the **console** link in the green message bar.

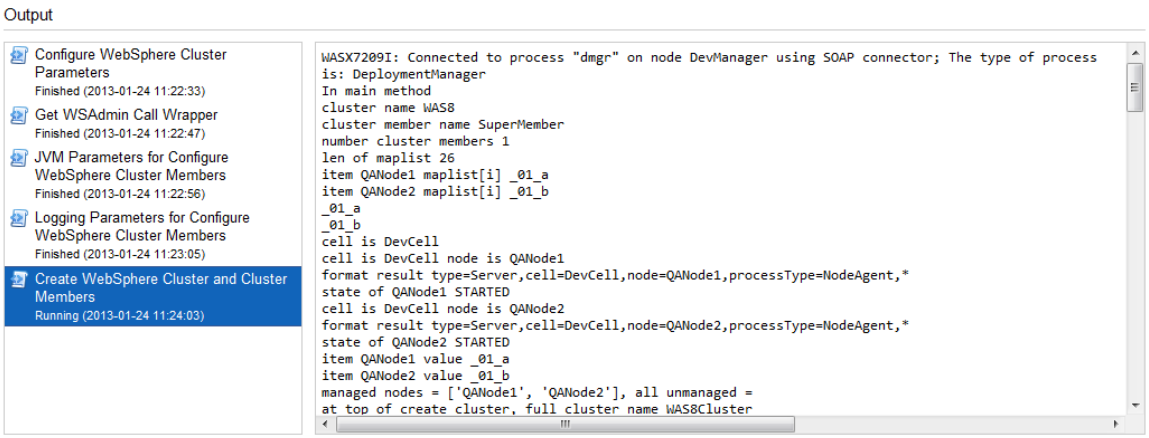
View the Results

While your workflow is running, you can watch its progress on the Automation > Console page.

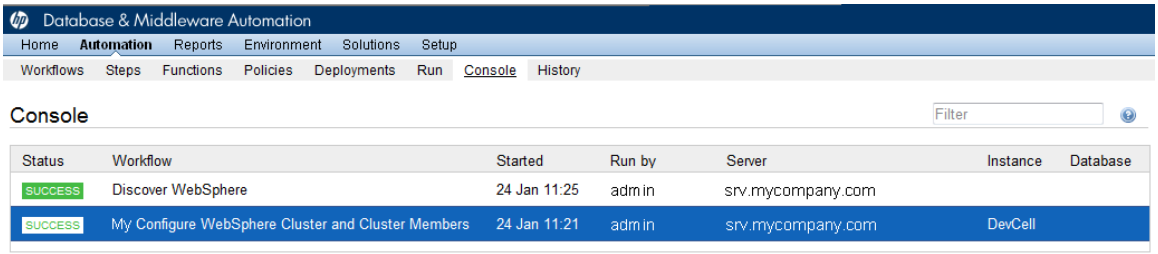
To view the progress of the workflow as the deployment proceeds, click the workflow name in the upper box on the Console page.



To view the outcome of a specific step, select that step in the left box in the Output area. Informational messages are displayed in the right box, and the values of any output parameters are listed.

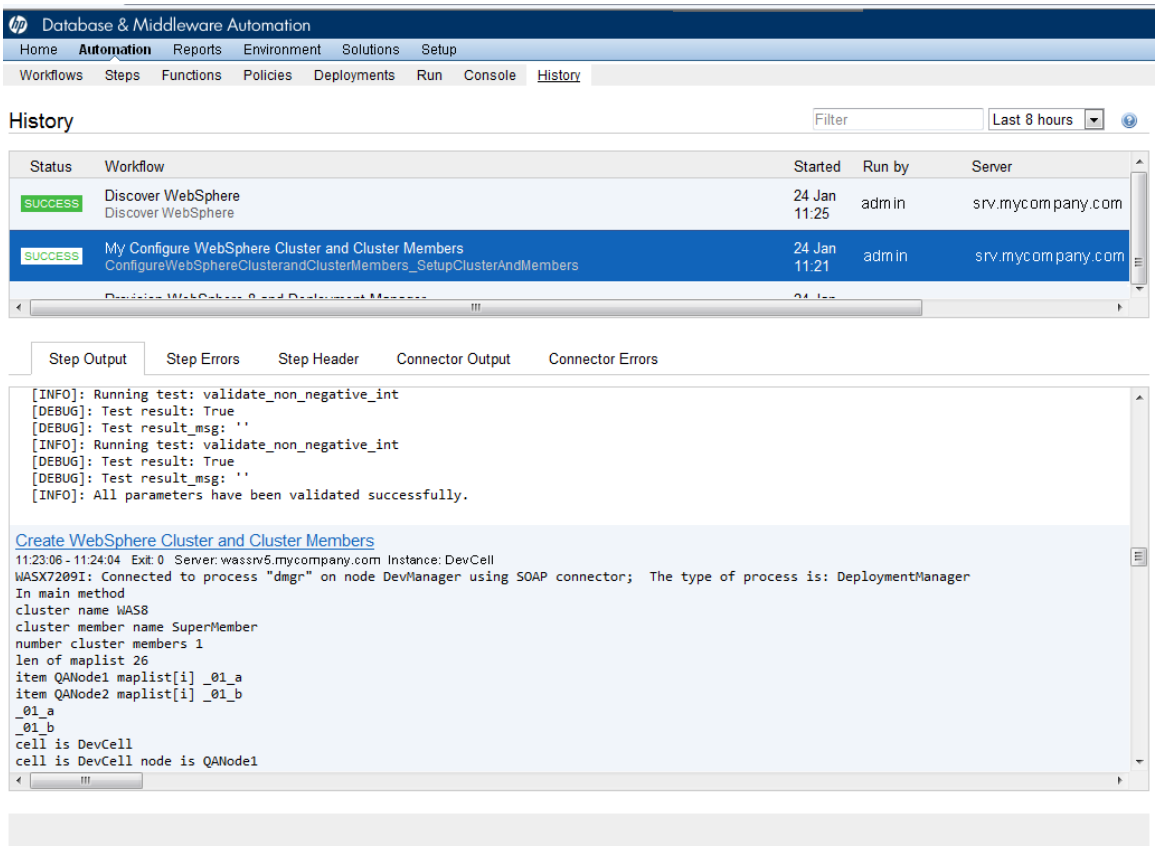


While the workflow is running, its status indicator on the Console says RUNNING. After the workflow finishes, its status indicator changes to SUCCESS, FAILURE, or FINISHED depending on the outcome of the workflow.



After the workflow has finished running, you can view a summary of your deployment on the History page. This page lists all the workflows that have run on this HP DMA server during the time period specified in the Filter box.

To view step-by-step results, select the row in the table that corresponds to your deployment.



The tabs below the table show you information about each step in the workflow. This includes the start and end time for each step, the exit code, and the following information:

- Step Output – any informational messages that were produced
- Step Errors – any errors that were reported
- Step Header – values assigned to any output parameters
- Connector Output – any informational messages related to the connection to your server management tool
- Connector Errors – any errors that were reported by the connector to your server management tool—if any errors were reported a red asterisk (*) appears on the tab

Chapter 3

Workflow Details

The Application Server Configuration Management solution pack contains the following WebSphere configuration management workflows. You can run these workflows ad-hoc for custom WebSphere installations or create reusable deployments to standardize WebSphere installations in your environment.

Workflow Name	Purpose
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.
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.
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.

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 configuration management 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 Use this Workflow" topic associated with each workflow.

The information presented here assumes the following:

- HP DMA is installed and operational.

- At least one suitable target server is available (see Supported Products and Platforms on page 13).
- You are logged in to the HP 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 described in the "Parameters" topic associated with each workflow.

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.

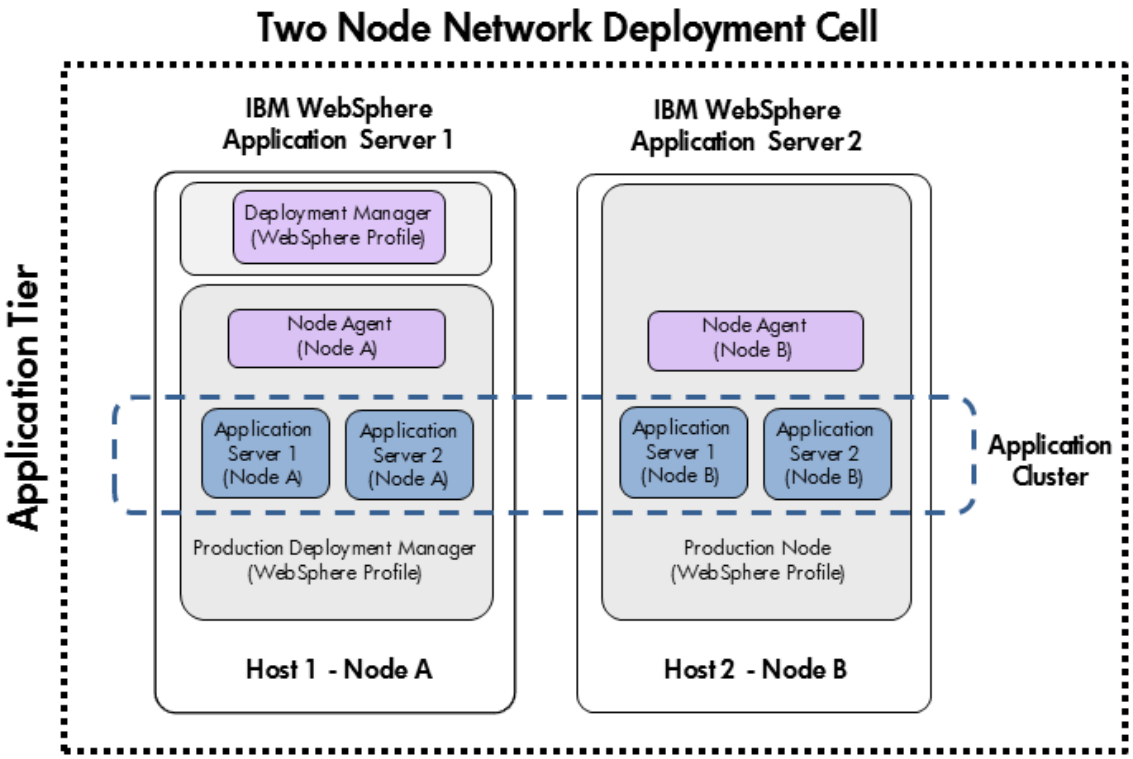
The cluster members are configured consistently based on a set of configurable parameters. If you do not specify parameters then the default WebSphere values are used.

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 WebSphere 7 or WebSphere 8.

Dependencies

This workflow has the following dependencies:

- You must have a working WebSphere Network Deployment cell version 7 or 8, with the Deployment Manager available for communication.
- You must run the Discover WebSphere workflow before you run the configuration management 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 HP DMA environment.

For more information about prerequisites for WebSphere, refer to the WebSphere Product Documentation on page 85.

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.

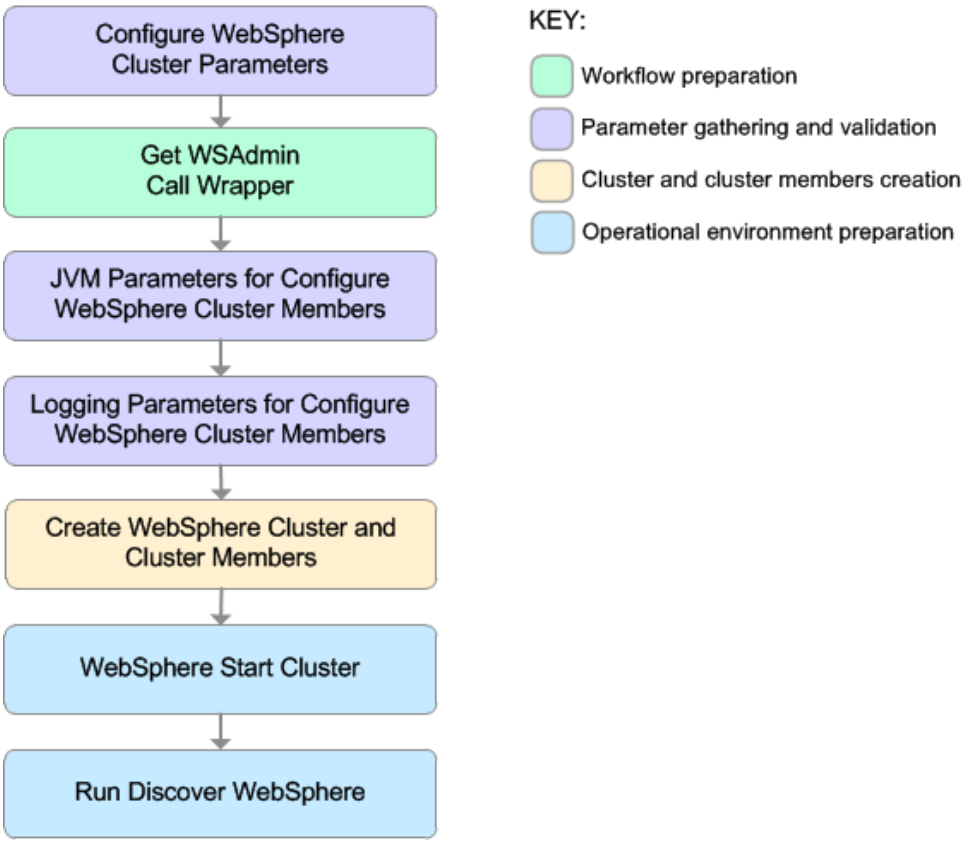
Validation Checks Performed

The workflow then performs the following checks on the input parameters:

WebSphere Admin Username	Cannot contain the following characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { } Cannot begin with a dash (-), period (.), or space ( )
WebSphere Admin Password	Cannot begin with a dash (-) Cannot contain a space ( )
Cluster Name Cluster Member Name	Must be specified Cannot contain the following characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { } 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 WebSphere Dmgr Host	Must be found in the metadata
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 `wsadmin` call wrapper.
Get WSAdmin Call Wrapper	This step creates the necessary call wrapper to call `wsadmin` 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 sure it started correctly.
Run Discover WebSphere	This step runs Discover WebSphere to examines the target server's physical environment to discover information about WebSphere cells, clusters, and application servers. **Note:** Discovery is ONLY additive. It will not remove instances or databases currently in your environment. It is your HP DMA administrator's responsibility to delete content that is no longer in use.

For parameter descriptions and defaults, see Parameters for Configure WebSphere Cluster and Cluster Members on page 45.

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 45.

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 (see Create a Deployable Workflow on page 19).
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.
Number Cluster Members	no default	required	The number of cluster members/application servers that will be created on each node.

Input Parameters for Configure WebSphere Cluster Parameters (continued)

Parameter Name	Default Value	Required	Description
Web Service Password	no default	required	Password for the HP DMA Discovery web service API.
Web Service URL	no default	required	URL for the HP DMA Discovery web service API. For example: `https://example.com:8443/dma`
Web Service User	no default	required	User capable of modifying the managed environment by using the HP DMA Discovery 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 / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }.

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 93).

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 Configure WebSphere Cluster and Cluster Members on page 45 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 (see Create a Deployment on page 20 for instructions).
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 (see Run Your Workflow on page 22 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.

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 45.

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 93).

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 HP DMA Discovery web service API.
Web Service URL	see description	URL for the HP DMA Discovery web service API. For example: `https://example.com:8443/dma`

Input Parameters for Configure WebSphere Cluster Parameters (continued)

Parameter Name	Example Value	Description
Web Service User	JohnDoe	User capable of modifying the managed environment by using the HP DMA Discovery 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 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. See How to Expose Additional Workflow Parameters on page 92. 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 HP DMA Discovery web service API.
Web Service URL	see description	URL for the HP DMA Discovery web service API. For example: `https://example.com:8443/dma`

Input Parameters for Configure WebSphere Cluster Parameters (continued)

Parameter Name	Example Value	Description
Web Service User	JohnDoe	User capable of modifying the managed environment by using the HP DMA Discovery 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 / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }.

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. See How to Expose Additional Workflow Parameters on page 92. 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 HP DMA Discovery web service API.
Web Service URL	see description	URL for the HP DMA Discovery web service API. For example: `https://example.com:8443/dma`
Web Service User	JohnDoe	User capable of modifying the managed environment by using the HP DMA Discovery 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: `/app/logs`
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. See How to Expose Additional Workflow Parameters on page 92. 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 HP DMA Discovery web service API.
Web Service URL	see description	URL for the HP DMA Discovery web service API. For example: `https://example.com:8443/dma`
Web Service User	JohnDoe	User capable of modifying the managed environment by using the HP DMA Discovery 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: `/app/logs`
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 (see How to Expose Additional Workflow Parameters on page 92). 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 HP DMA Discovery web service API.
Web Service URL	no default	required	URL for the HP DMA Discovery web service API. For example: `https://example.com:8443/dma`
Web Service User	no default	required	User capable of modifying the managed environment by using the HP DMA Discovery 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 ( ).

Parameters Defined in this Step: Configure WebSphere Cluster Parameters (continued)

Parameter Name	Default Value	Required	Description
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.

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

See WebSphere Product Documentation on page 1 to find IBM documentation for the supported database versions. See Database Product Documentation on page 85 to find additional information about the supported databases.

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 or WebSphere 8.

Dependencies

This workflow has the following dependencies:

- You must have a working WebSphere Network Deployment cell version 7 or 8, with the Deployment Manager available for communication.
- You must run the Discover WebSphere workflow before you run the configuration management 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 HP 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 Product Documentation on page 85.

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:

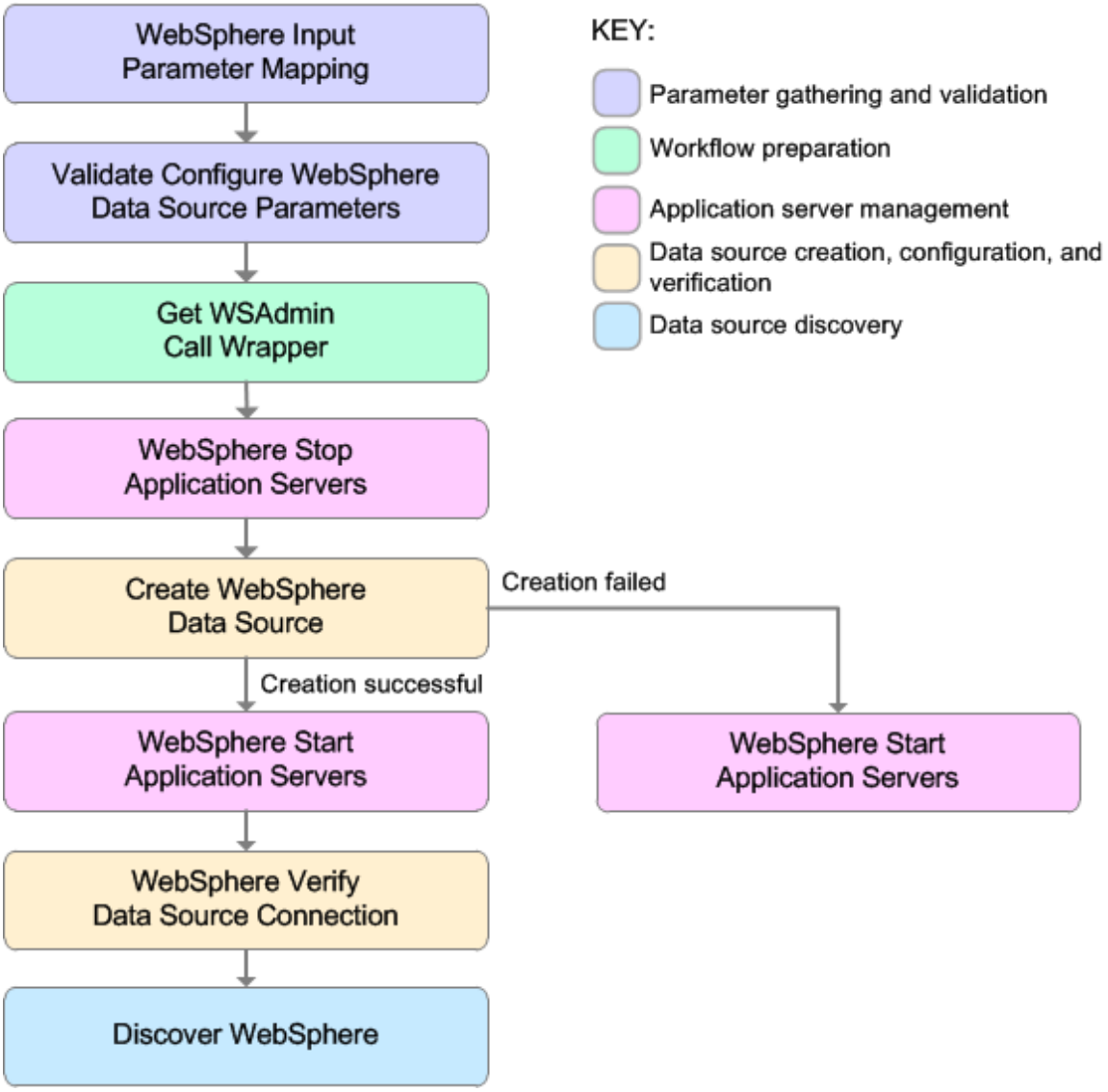
WebSphere Admin Username	Cannot contain the following characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { } Cannot begin with a dash (-), period (.), or space ( )
WebSphere Admin Password	Cannot begin with a dash (-) Cannot contain a space ( )
Enable Security	Must be true or false
If Enable Security 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
Trust SSL Certificates 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	This step performs the following actions to facilitate the execution of subsequent steps in the workflow: 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	This step prepares and validates the parameters needed to configure a JDBC provider, J2C alias, and data source for a WebSphere Application Server.
Get WSAdmin Call Wrapper	This step creates the necessary call wrapper to call `wsadmin` to execute certain operations within a given WebSphere environment.
WebSphere Stop Application Servers	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.
Create WebSphere Data Source	This step creates and configures the JDBC provider, J2C alias, and data source within a WebSphere Application Server scope.
WebSphere Start Application Servers	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.
WebSphere Verify Data Source Connection	This step verifies the connection of a newly created data source within WebSphere.
Discover WebSphere	This step audits the server's physical environment looking for WebSphere cells, clusters, and application servers. **Note:** Discovery is ONLY additive. It will not remove instances or databases currently in your environment. It is your HP DMA administrator's responsibility to delete content that is no longer in use.

For parameter descriptions and defaults, see Parameters for Create and Configure WebSphere Data Sources on page 67.

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 67.

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 (see Create a Deployable Workflow on page 19).
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 if 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`

Input Parameters for Validate Configure WebSphere Data Source Parameters (continued)

Parameter Name	Default Value	Required	Description
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`
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.

Input Parameters for Validate Configure WebSphere Data Source Parameters (continued)

Parameter Name	Default Value	Required	Description
Trust SSL Certificates	True	optional	Indicates whether to trust any SSL certificate used to connect to the HP DMA web service. Valid values are True or False.
Web Service Password	no default	required	Password for the HP DMA Discovery web service API.
Web Service User	no default	required	User capable of modifying the managed environment by using the HP DMA Discovery 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 / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }.

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 93).

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 Create and Configure WebSphere Data Sources on page 67 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 (see Create a Deployment on page 20 for instructions).
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 (see Run Your Workflow on page 22 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.

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 67.

The sample scenarios assume that Web Service URL has the value of DMA.url. This is the default value mapped from the HP DMA metadata.

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 93).

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 and does not trust SSL certificates.

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.

Input Parameters for Validate Configure WebSphere Data Source Parameters (continued)

Parameter Name	Example Value	Description
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.
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.
Trust SSL Certificates	False	Indicates whether to trust any SSL certificate used to connect to the HP DMA web service. Valid values are True or False.
Web Service Password	myWebSvcPwd	Password for the HP DMA Discovery web service API.
Web Service User	JohnDoe	User capable of modifying the managed environment by using the HP DMA Discovery web service API.

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 will trust SSL certificates. This example 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 if 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/sqlserver/jdbc/sqljdbc4.jar` for UNIX and `C:\app\sqlserver\jdbc\sqljdbc4.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.

Input Parameters for Validate Configure WebSphere Data Source Parameters (continued)

Parameter Name	Example Value	Description
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.
Trust SSL Certificates	True	Indicates whether to trust any SSL certificate used to connect to the HP DMA web service. Valid values are True or False.
Web Service Password	myWebSvcPwd	Password for the HP DMA Discovery web service API.
Web Service User	JohnDoe	User capable of modifying the managed environment by using the HP DMA Discovery web service API.

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. This example does not trust SSL certificates.

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`

Input Parameters for Validate Configure WebSphere Data Source Parameters (continued)

Parameter Name	Example Value	Description
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.
Trust SSL Certificates	False	Indicates whether to trust any SSL certificate used to connect to the HP DMA web service. Valid values are True or False.
Web Service Password	myWebSvcPwd	Password for the HP DMA Discovery web service API.
Web Service User	JohnDoe	User capable of modifying the managed environment by using the HP DMA Discovery 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 trust SSL certificates and does not enable security.

Note: Some of these parameters are not exposed by default in the deployment. See How to Expose Additional Workflow Parameters on page 92. 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 if 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/sqlserver/jdbc/sqljdbc4.jar` for UNIX and `C:\app\sqlserver\jdbc\sqljdbc4.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.

Input Parameters for Validate Configure WebSphere Data Source Parameters (continued)

Parameter Name	Example Value	Description
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 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.
Trust SSL Certificates	False	Indicates whether to trust any SSL certificate used to connect to the HP DMA web service. Valid values are True or False.
Web Service Password	myWebSvcPwd	Password for the HP DMA Discovery web service API.
Web Service User	JohnDoe	User capable of modifying the managed environment by using the HP DMA Discovery 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 (see How to Expose Additional Workflow Parameters on page 92). 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 if 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.

Parameters Defined in this Step: Validate Configure WebSphere Data Source Parameters (continued)

Parameter Name	Default Value	Required	Description
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`
Maximum Pool Connections	see descriptioin	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.
Trust SSL Certificates	True	optional	Indicates whether to trust any SSL certificate used to connect to the HP DMA web service. Valid values are True or False.
Web Service Password	no default	required	Password for the HP DMA Discovery web service API.

Parameters Defined in this Step: Validate Configure WebSphere Data Source Parameters (continued)

Parameter Name	Default Value	Required	Description
Web Service URL	see description	required	URL for the HP DMA Discovery web service API. For example: `https://example.com:8443/dma` By default this is mapped to DMA.Url. You can also set this in a policy (see How to Use a Policy to Specify Parameter Values).
Web Service User	no default	required	User capable of modifying the managed environment by using the HP DMA Discovery 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.

See WebSphere Product Documentation on page 1 to find IBM documentation for 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 or WebSphere 8.

Dependencies

This workflow has the following dependencies:

- You must have a working WebSphere Network Deployment cell version 7 or 8, with the Deployment Manager available for communication.
- You must run the Discover WebSphere workflow before you run the configuration management 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 HP DMA environment.

For more information about prerequisites for WebSphere, refer to the WebSphere Product Documentation on page 85.

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.

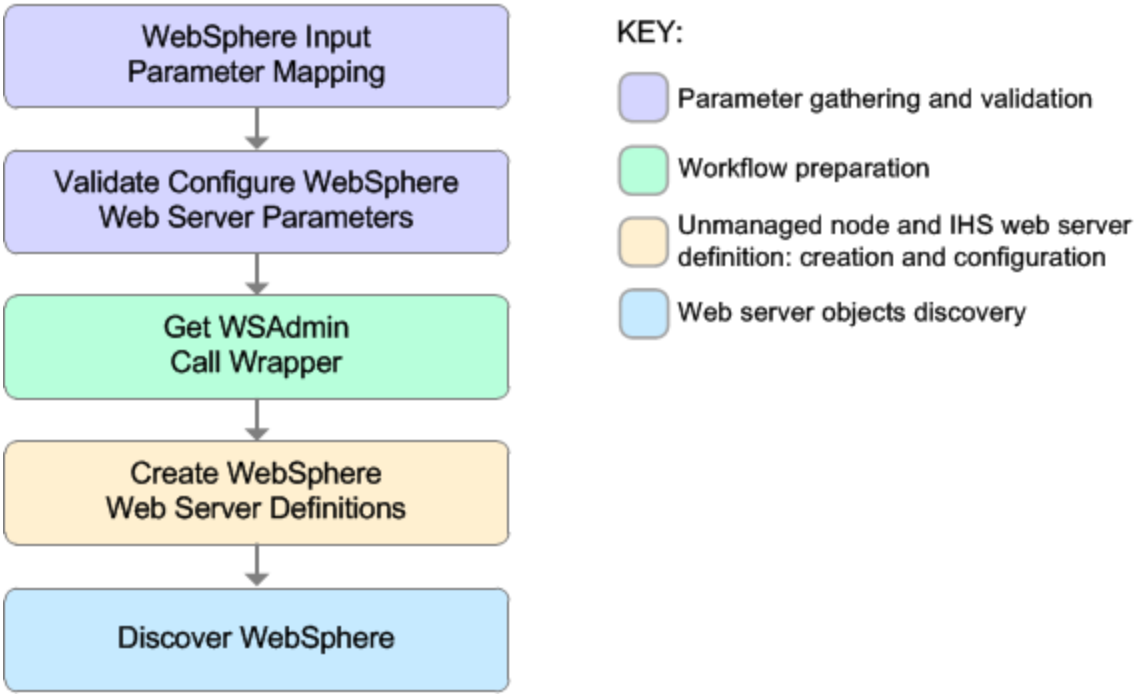
Validation Checks Performed

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 (-) Cannot contain a space ( )
HTTP Admin User	Cannot contain the following characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { } 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 / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { } Cannot begin with a dash (-), period (.), or space ( )
WebSphere Admin Password	Cannot begin with a dash (-) 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
Trust SSL Certificates 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	This step performs the following actions to facilitate the execution of subsequent steps in the workflow: 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	This step prepares and validates the parameters needed to create and configure an unmanaged node and create an IHS web server definition.
Get WSAdmin Call Wrapper	This step creates the necessary call wrapper to call `wsadmin` to execute certain operations within a given WebSphere environment.
Create WebSphere Web Server Definitions	This step creates and configures the WebSphere unmanaged node and IHS web server definition.
Discover WebSphere	This step audits the server's physical environment looking for WebSphere cells, clusters, and application servers. **Note:** Discovery is ONLY additive. It will not remove instances or databases currently in your environment. It is your HP DMA administrator's responsibility to delete content that is no longer in use.

For parameter descriptions and defaults, see Parameters for Create and Configure WebSphere Web Server Definitions on page 83.

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 (see Create a Deployable Workflow on page 19).
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`

Input Parameters for Validate Configure WebSphere Web Server Parameters (continued)

Parameter Name	Default Value	Required	Description
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: `/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	True	optional	Indicates whether to trust any SSL certificate used to connect to the HP DMA web service. Valid values are 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 HP DMA Discovery web service API.
Web Service User	no default	required	User capable of modifying the managed environment by using the HP DMA Discovery web service API.

Input Parameters for Validate Configure WebSphere Web Server Parameters (continued)

Parameter Name	Default Value	Required	Description
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 / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }.

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 93).

Note: See Parameters for Create and Configure WebSphere Web Server Definitions on page 83 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 (see Create a Deployment on page 20 for instructions).
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 (see Run Your Workflow on page 22 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.

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 83.

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 93).

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
- Trusts SSL certificates
- 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.

Input Parameters for Validate Configure WebSphere Web Server Parameters (continued)

Parameter Name	Example Value	Description
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.
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`
Trust SSL Certificates	True	Indicates whether to trust any SSL certificate used to connect to the HP DMA web service. Valid values are True or False.
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 HP DMA Discovery web service API.
Web Service User	JohnDoe	User capable of modifying the managed environment by using the HP DMA Discovery 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
- Does not trust SSL certificates
- 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: `/opt/IBM/HTTPServer/logs/access.log`
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: `/opt/IBM/HTTPServer/logs/error.log`
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	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	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.

Input Parameters for Validate Configure WebSphere Web Server Parameters (continued)

Parameter Name	Example Value	Description
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: `/opt/IBM/HTTPServer/Plugin`
Trust SSL Certificates	False	Indicates whether to trust any SSL certificate used to connect to the HP DMA web service. Valid values are True or False.
Unmanaged Node Host Name	see description	Host name of the system associated with the node specified in Unmanaged Node Name.
Unmanaged Node Name	webServerNode	The node name in the configuration repository.
WebApp Mapping	ALL	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 HP DMA Discovery web service API.
Web Service User	JohnDoe	User capable of modifying the managed environment by using the HP DMA Discovery 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 / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }.

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: `/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.
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.

Parameters Defined in this Step: Validate Configure WebSphere Web Server Parameters (continued)

Parameter Name	Default Value	Required	Description
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	True	optional	Indicates whether to trust any SSL certificate used to connect to the HP DMA web service. Valid values are 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 HP DMA Discovery web service API.
Web Service User	no default	required	User capable of modifying the managed environment by using the HP DMA Discovery 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 / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }.

Chapter 4

Reference Information

This chapter contains the following information:

Topic	Description
WebSphere Product Documentation	Links to product documentation for IBM WebSphere Application Server Network Deployment (WebSphere), the hardware and software requirements, as well as supported platforms
Database Product Documentation	Links to product documentation for the database products that these workflows support
HP DMA Documentation	Links to additional HP DMA documentation

WebSphere Product Documentation

For the current list of hardware and software requirements, as well as supported platforms for IBM HTTP Server, see:

http://www-01.ibm.com/support/docview.wss?uid=swg27006921

For WebSphere 7 product documentation, see:

http://publib.boulder.ibm.com/infocenter/wasinfo/v7r0/index.jsp

For WebSphere 8 product documentation, see:

http://publib.boulder.ibm.com/infocenter/wasinfo/v8r0/index.jsp

For IBM Red Book resources for WebSphere, see:

http://publib-b.boulder.ibm.com/Redbooks.nsf/portals/WebSphere

Note: The links to the documents listed here were correct as of the publication of this guide.

Database Product Documentation

The following topics contain links to documentation for the database products supported by this solution:

Note: The links to the documents listed here were correct as of the publication of this guide.

Oracle Database Product Documentation

The product documentation for Oracle Database Enterprise Edition version 11g is located here:

http://www.oracle.com/pls/db112/homepage

Microsoft SQL Server Documentation

For information about SQL Server, including prerequisites, see the Microsoft SQL Server documentation available at the following web site:

http://msdn.microsoft.com/en-us/library/ms143506.aspx

HP DMA Documentation

For information about using the HP DMA web interface, see the *HP DMA User Guide* and the *HP DMA Administrator Guide*.

These documents are part of the HP DMA documentation library, which is available on the HP Software Product Manuals web site:

http://h20230.www2.hp.com/selfsolve/manuals

Chapter 5

Tips and Best Practices

This portion of the document contains a collection of tips and best practices that will enable you to use HP DMA more effectively. It contains the following topics:

How a Solution Pack is Organized on the next page

How to Expose Additional Workflow Parameters on page 92

How to Use a Policy to Specify Parameter Values on page 93

How to Import a File into the Software Repository on page 96

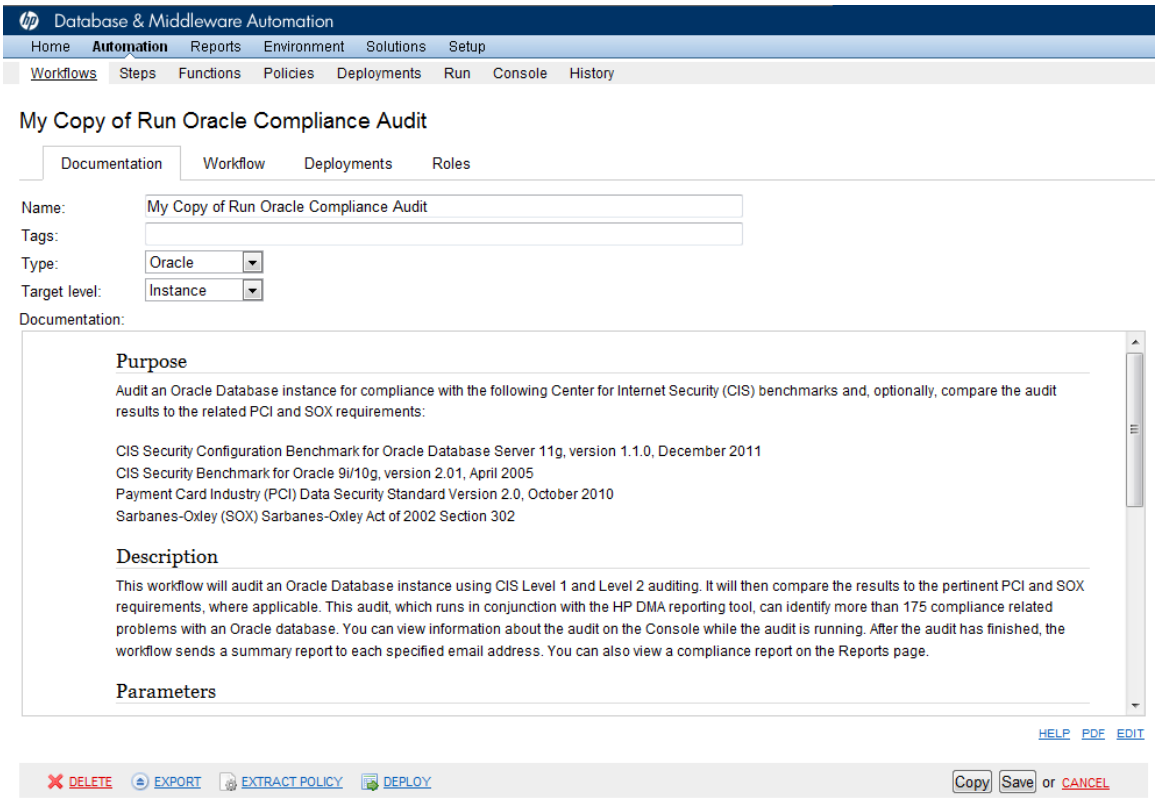
How a Solution Pack is Organized

Note: This topic uses the Run Oracle Compliance Audit workflow in the Database Compliance solution pack as an example. The information provided here, however, pertains to any solution pack.

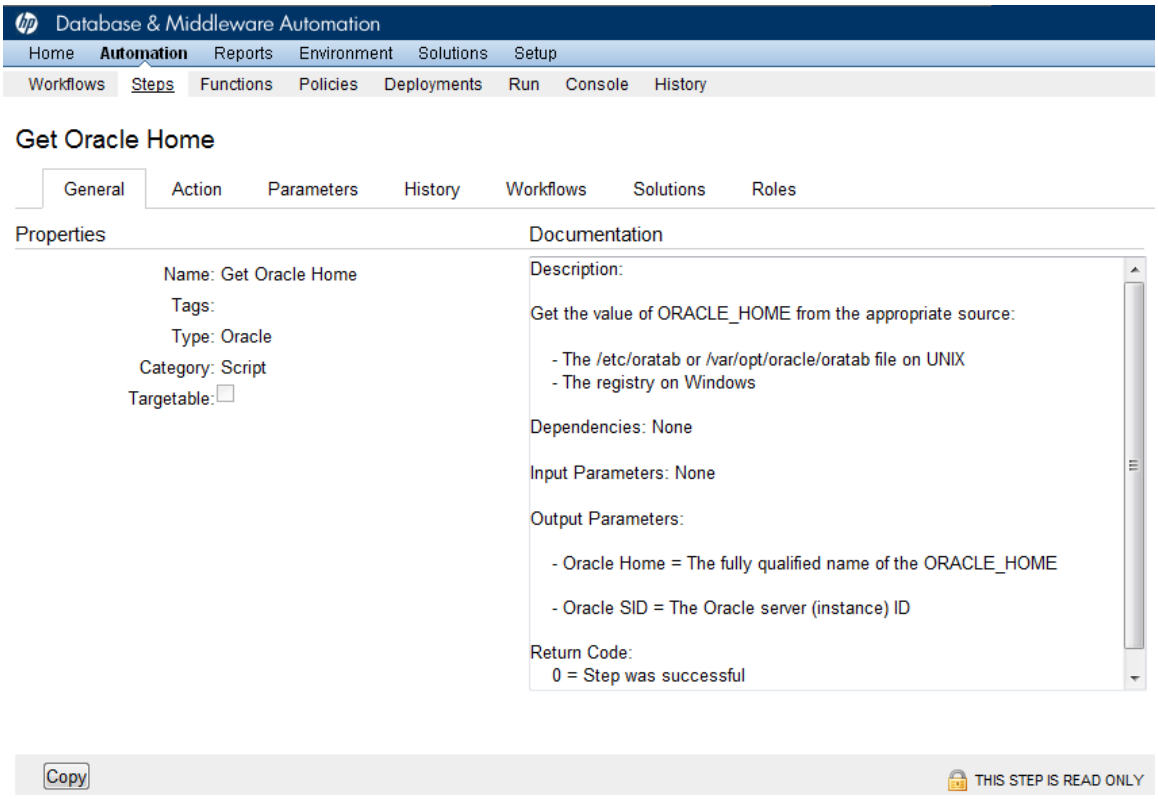
In HP DMA, a **workflow** executes a process —such as installing a software product or checking a database instance for compliance with a specific security benchmark.

A **solution pack** contains one or more related **workflow templates**.

Each workflow template has a Documentation tab that provides detailed information about that workflow.

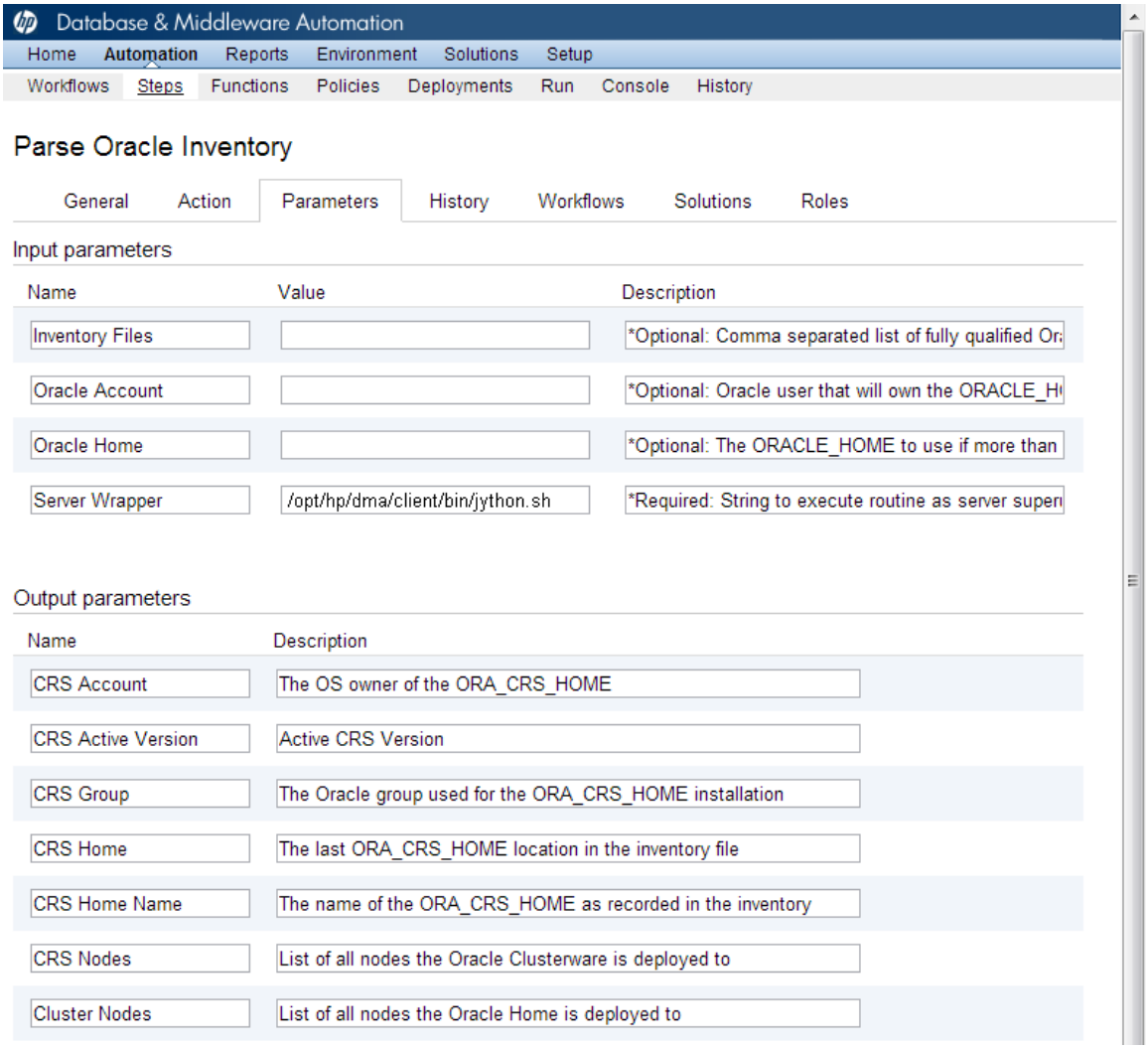


A workflow consists of a sequence of **steps**. Each step performs a very specific task. Each step includes a documentation panel that briefly describes its function.

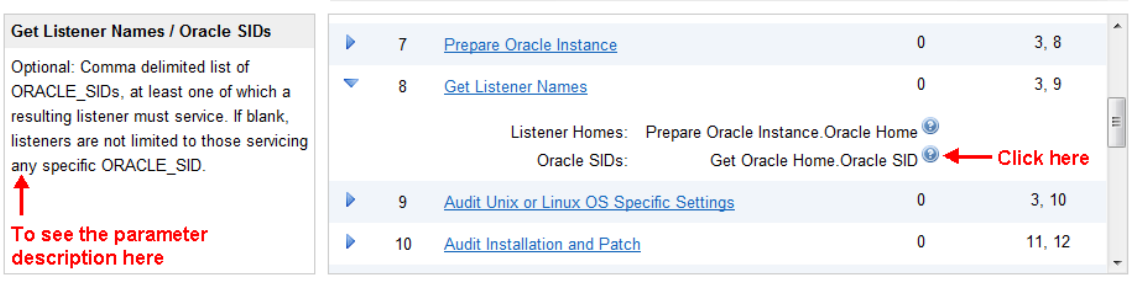


Steps can have input and output **parameters**. Output parameters from one step often serve as input parameters to another step. Steps can be shared among workflows.

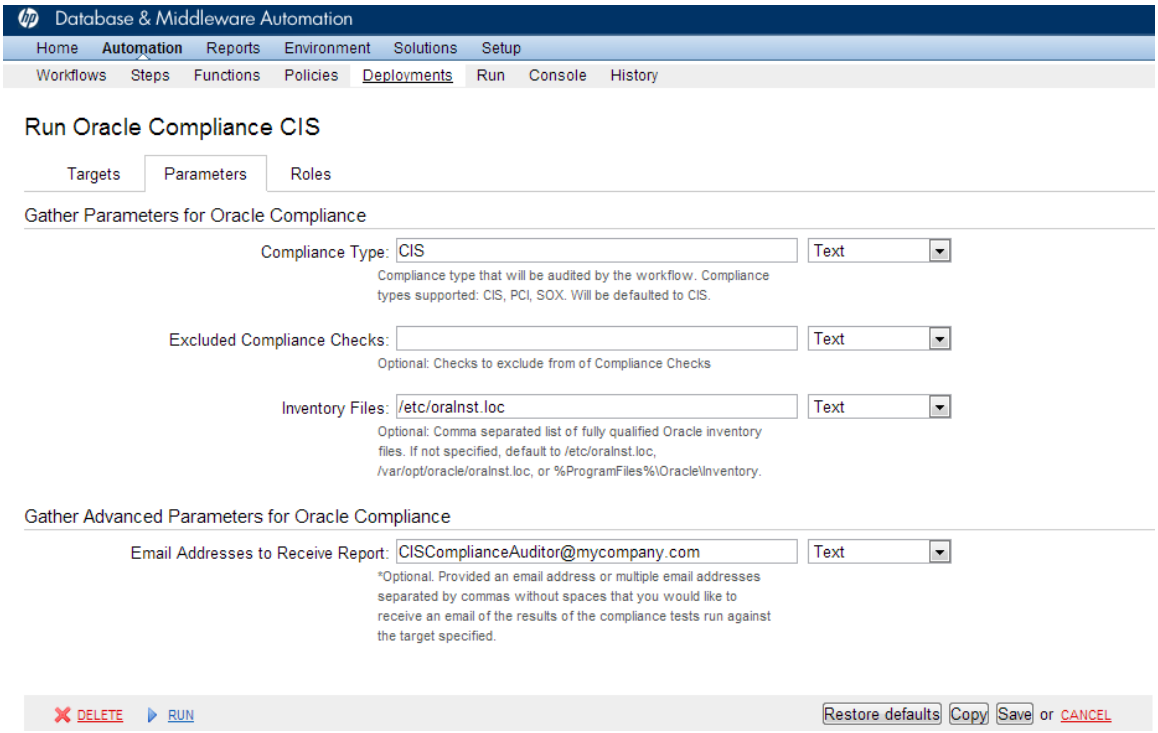
Parameter descriptions are displayed on the Parameters tab for each step in the workflow.



Parameter descriptions are also displayed on the Workflow tab for each workflow.



Parameter descriptions are also displayed on the Parameters tab in the **deployment** (organized by step).



Note: The workflow templates included in this solution pack are read-only and cannot be deployed. To use a workflow template, you must first create a copy of the template and then customize that copy for your environment.

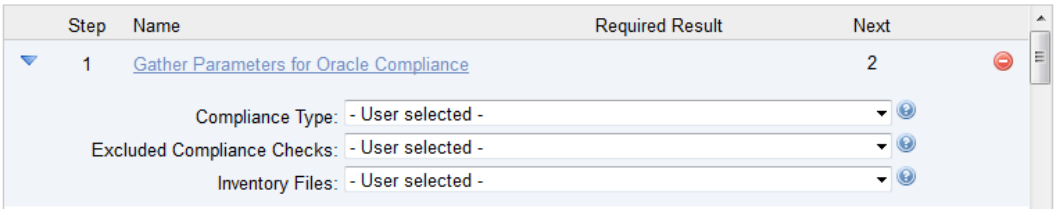
How to Expose Additional Workflow Parameters

Each workflow in this solution pack has a set of input parameters. Some are required and some are optional. To run a workflow in your environment, you must specify values for a subset of these parameters when you create a deployment.

By default, only a few of the input parameters for each workflow are visible on the Deployment page, and the rest are hidden. In order to specify a value for a parameter that is currently hidden, you must first expose that parameter by changing its mapping in the workflow editor.

To expose a hidden workflow parameter:

1. In the HP DMA web interface, go to Automation > Workflows.
2. From the list of workflows, select a deployable workflow.
3. Go to the Workflow tab.
4. In the list of steps below the workflow diagram, click the ▶ (blue arrow) to the immediate left of the pertinent step name. This expands the list of input parameters for this step.
5. For the parameter that you want to expose, select - User Selected - from the drop-down list. For example:



6. Repeat steps 4 and 5 for all the parameters that you would like to specify in the deployment.
7. Click **Save** in the lower right corner.

How to Use a Policy to Specify Parameter Values

It is sometimes advantageous to provide parameter values by using a policy rather than explicitly specifying the values in a deployment. This approach has the following advantages:

- The policy can be used in any deployment.
- It is faster and less error-prone than specifying parameter values manually.
- For parameter values that change frequently—for example, passwords that must be changed regularly—you only need to update them in one place.

To establish a policy, you can either Create a Policy or Extract a Policy from a workflow.

After you establish the policy, you must Reference the Policy in the Deployment.

For more information, see the *HP DMA User Guide*. This document is available on the HP Software Product Manuals web site: http://h20230.www2.hp.com/selfsolve/manuals

Create a Policy

The first step in this approach is to create a policy that provides parameter values. There are two ways to do this: (1) create a new policy, and define all attributes manually (as shown here) or (2) extract a policy from a workflow (see Extract a Policy on the next page).

To create a policy that provides parameter values:

1. In the HP DMA web UI, go to Automation > Policies.
2. Click **New Policy**.
3. In the **Name** box, specify the name of the policy
4. For each parameter value that you want to provide using this policy, perform the following actions on the Attributes tab:
   a. From the drop-down list, select the type of attribute:
      - A Text attribute contains simple text that users can view while deploying and running workflows.
      - A List attribute contains a comma-separated list of values (or a large amount of text not suitable for a Text attribute).
      - A Password attribute contains simple text, but the characters are masked so that users cannot see the text.

   b. In the text box to the left of the Add button, specify the name of the attribute.

      For your convenience, this name should be similar to the parameter name used in the pertinent workflow (or workflows).

   c. Click **Add**.

   d. In the new text box to the right of the attribute's name, enter a value for this attribute.

      To remove an attribute, click the **Remove** button.
5. On the Roles tab, grant Read and Write permission to any additional users and groups who will

be using this policy. By default, any groups to which you belong have Read and Write permission.

6. Click the **Save** button (lower right corner).

Extract a Policy

An alternative to creating your own policy one attribute at a time is to extract the policy. This automatically creates 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 screen.
4. Specify values for each attribute listed.
5. *Optional:* Remove any attributes that you do not want to use.
6. *Optional:* Add any new attributes that you 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**.

Reference the Policy in the Deployment

After you create a policy, you can reference its attributes in a deployment.

To reference policy attributes in a deployment:

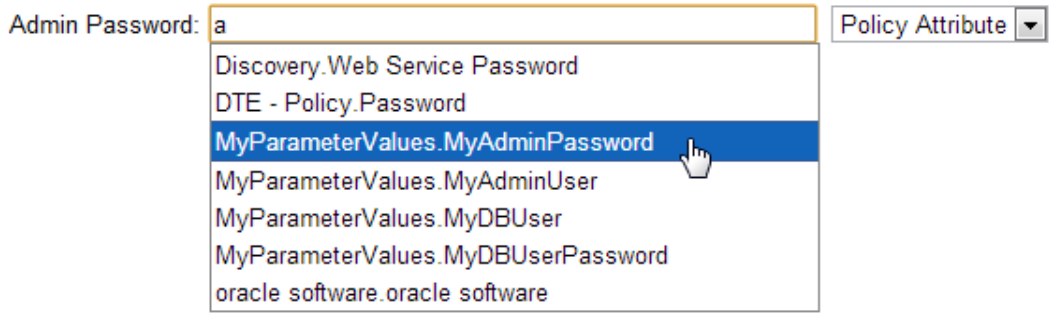
1. Create or access the deployment.

   See “Deployments” in the *HP DMA User Guide* for details.

2. On the Parameters tab, perform the following steps for each parameter whose value you want to provide by referencing a policy attribute:

   a. In the drop-down menu for that parameter, select **Policy Attribute**.

   b. In the text box for that parameter, type any character. A drop-down list of policy attributes appears. For example:



c. From the drop-down list, select the attribute that you want to reference. For example:

3. Click **Save** to save your changes to the deployment.

How to Import a File into the Software Repository

Many HP DMA workflows are capable of downloading files from the software repository on the HP DMA server to the target server (or servers) where the workflow is running. The following procedure shows you how to import a file into the software repository so that it can be downloaded and deployed by a workflow.

HP DMA uses the HP Server Automation (HP SA) Software Library as its software repository.

Tip: Be sure to use unique file names for all files that you import into the software repository.

To import a file into the HP SA Software Library:

1. Launch the HP SA Client from the Windows Start Menu.

   By default, the HP SA Client is located in Start → All Programs → HP Software → HP Server Automation Client

   If the HP SA Client is not installed locally, follow the instructions under "Download and Install the HP SA Client Launcher" in the *HP Server Automation Single-Host Installation Guide*.
2. In the navigation pane in the HP SA Client, select Library → By Folder.
3. Select (or create) the folder where you want to store the file.
4. From the Actions menu, select **Import Software**.
5. In the Import Software dialog, click the **Browse** button to the right of the File(s) box.
6. In the Open dialog:
   a. Select the file (or files) to import.
   b. Specify the character encoding to be used from the Encoding drop-down list. The default encoding is English ASCII.
   c. Click **Open**. The Import Software dialog reappears.
7. From the Type drop-down list, select **Unknown**.
8. If the folder where you want to store the files does not appear in the Folder box, follow these steps:
   a. Click the **Browse** button to the right of the Folder box.
   b. In the Select Folder window, select the import destination location, and click **Select**. The Import Software dialog reappears.
9. From the Platform drop-down list, select all the operating systems listed.
10. Click **Import**.

    If one of the files that you are importing already exists in the folder that you specified, you will be prompted regarding how to handle the duplicate file. Press F1 to view online help that explains the options.
11. Click **Close** after the import is completed.

Chapter 6

Troubleshooting

These topics can help you address problems that might occur when you install and run the workflows in this solution pack:

- Target Type below
- User Permissions and Related Requirements below
- Discovery in HP DMA on the next page

Target Type

In your deployment, make sure that you have specified the correct type of target. The workflow type and the target type must match. A workflow designed to run against an instance target, for example, cannot run against a server target.

User Permissions and Related Requirements

Roles define access permissions for organizations, workflows, steps, policies, and deployments. Users are assigned to roles, and they gain access to these automation items according to the permissions and capabilities defined for their roles.

Roles are assigned by your server management tool administrator. They are then registered in HP DMA by your HP DMA administrator.

Your HP DMA administrator will ensure that the users in your environment are assigned roles that grant them the permissions and capabilities they need to accomplish their tasks. For example:

- To create a workflow, your role must have Workflow Creator capability.
- To view a workflow, your role must have Read permission for that workflow.
- To edit a workflow, your role must have Write permission for that workflow.
- To view a deployment, your role must have Read permission for that deployment.
- To modify a deployment, your role must have Write permission for that deployment.
- To run a deployment, your role must have Execute permission for that deployment and Deploy permission for the organization where it will run.

Capabilities determine what features and functions are available and active in the HP DMA UI for each user role.

For more information, see the *HP DMA Administrator Guide*. This document is available on the HP Software Product Manuals web site: http://h20230.www2.hp.com/selfsolve/manuals

Discovery in HP DMA

HP DMA uses a process called “discovery” to find information about the servers, networks, and database instances on target machines in your managed environment.

You must explicitly initiate the process of discovery—it is not automatic. See the *HP DMA User Guide* for instructions. This document is available on the HP Software Product Manuals web site: http://h20230.www2.hp.com/selfsolve/manuals

Glossary

A

automation items

The umbrella term automation items is used to refer to those items to which role-based permissions can be assigned. Automation items include workflows, deployments, steps, and policies.

B

bridged execution

A bridged execution workflow includes some steps that run on certain targets and other steps that run on different targets. An example of a bridged execution workflow is Extract and Refresh Oracle Database via RMAN (in the Database Refresh solution pack). This workflow extracts the contents of a database on one target (the Source) and creates a new database with the same contents on another target (the Destination). This workflow is useful when you want to clone a database - for example, to move it from a traditional IT infrastructure location into a private cloud. Bridged execution workflows are supported on HP DMA version 9.11 (and later).

C

capability

Capabilities are collections of related privileges. There are three capabilities defined in HP DMA. Login Access capability enables a user to log in to the web interface. This capability does not guarantee that this user can view any organizations or automation items—permissions are required to access those items. Workflow Creator capability enables a user to create new workflows and make copies of other workflows. Administrator capability enables a user to perform any action and view all organizations. If you have Administrator capability, you do not need Workflow Creator capability. The Administrator can assign any of these capabilities to one or more roles registered roles.

connector

HP DMA includes a Connector component that enables it to communicate with your server management tool. You must configure the Connector before you can run an workflow against a target.

cross-platform

Cross-platform database refresh involves converting the data from one type of byte ordering to another. This is necessary, for example, if you want to load a database dump file on a little-endian Linux target that was created on a big-endian Solaris server.

custom field

Custom Fields are used to customize workflows or show information about the environment. Custom Fields can be used in workflow steps to automatically supply information that is specific to an organization, server, instance, or database.

D

deployment

Deployments associate a workflow with a target environment in which a workflow runs. You can customize a deployment by specifying values for any workflow parameters that are designated - User Selected - in the workflow. You must save a deployment before you can run the workflow. You can re-use a saved deployment as many times as you like.

F

function

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. Functions are “injected” into the step code just prior to step execution.

I

input parameters

A workflow has a set of required parameters for which you must specify a value. The required parameters are a subset of all the parameters associated with that workflow. The remaining parameters are considered optional. You can specify a value for an optional parameter by first exposing it using the workflow editor and then specifying the value when you create a deployment.

M

mapping

An input parameter is said to be "mapped" when it's value is linked to an output parameter from a previous step in the workflow or to a metadata field. Mapped parameters are not visible on the Deployment page. You can "unmap" a parameter by specifying - User Selected - in the workflow editor. This parameter will then become visible on the Deployment page.

O

organization

An organization is a logical grouping of servers. You can use organizations to separate development, staging, and production resources - or to separate logical business units.

P

parameters

Parameters are pieces of information - such as a file system path or a user name - that a step requires to carry out its action. Values for parameters that are designated User Selected in the workflow can be specified in the deployment. Parameters that are marked Enter at Runtime in the deployment must be specified on the target system when the workflow runs.

policy

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 HP DMA to manage groups of hundreds or thousands of servers at a time without the need to configure each individual server.

R

raw devices

In Sybase ASE version 15, you can create and mount database devices on raw bound devices. This enables Sybase ASE to use direct memory access from your address space to the physical sectors on the disk. This can improve performance by reducing memory copy operations from the user address space to the operating system kernel buffers.

role

Each HP DMA user has one or more roles. Roles are used to grant users permission to log in to and to access specific automation items and organizations. Roles are defined in your server management tool. Before you can associate a role with an automation item or organization, however, you must register that role in HP DMA.

S

smart group

Smart Groups are dynamic groups of servers, instances, or databases defined by some criteria. They are used to specify targets for deployments. As information about an environment object changes, its membership in the groups is re-evaluated.

software repository

The software repository is where the workflow will look for any required files that are not found on the target server. If you are using HP DMA with HP Server Automation (SA), this repository is the SA Software Library.

solution pack

A solution pack contains one or more related workflow templates. These templates are read-only and cannot be deployed. To run one of the workflows included in a solution pack, you must first create a deployable copy of that template and then customize that copy for your environment. Solution packs are organized by function - for example: database patching or application server provisioning.

steps

Steps contains the actual code used to perform a unit of work detailed in a workflow.

T

target instance

In the context of MS SQL database refresh, the term "target instance" refers to the SQL Server instance where the database that will be restored resides.

W

workflow

A workflow automates the process followed for an operational procedure. Workflows contain steps, which are linked together to form business logic for a common task. Workflows connect existing tasks in order to perform a new business process by building on existing best practices and processes.

workflow editor

The workflow editor is the tool that you use to assemble steps into workflows. You can map each input parameter to output parameters of previous steps or built-in metadata (such as the server name, instance name, or database name). You can also specify User Selected to expose a parameter in the deployment; this enables the person who creates the deployment to specify a value for that parameter.

workflow templates

A workflow template is a read-only workflow that cannot be deployed. To run one of the workflows included in a solution pack, you must first create a deployable copy of the workflow template and then customize that copy for your environment.