Hewlett Packard Enterprise

HPE Database and Middleware Automation

Ultimate Edition

Software Version: 10.40
Linux, Solaris, AIX, and HP-UX

Workflows for IBM WebSpehere

Document Release Date: December 2015
Software Release Date: December 2015

Legal Notices

Warranty

The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HPE 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 HPE 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

Trademark Notices

Adobe™ is a trademark of Adobe Systems Incorporated.

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

UNIX® is a registered trademark of The Open Group.

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

Documentation Updates

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, go to: **https://softwaresupport.hp.com**

This site requires that you register for an HP Passport and sign in. To register for an HP Passport ID, go to: **https://hpp12.passport.hp.com/hppcf/createuser.do**

Or click the **the Register** link at the top of the HPE Software Support page.

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

Support

Visit the HPE Software Support Online web site at: **https://softwaresupport.hp.com**

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

HPE 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 HPE 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:

https://hpp12.passport.hp.com/hppcf/createuser.do

To find more information about access levels, go to:

https://softwaresupport.hp.com/web/softwaresupport/access-levels

HP Software Solutions Now accesses the HPESW Solution and Integration Portal Web site. This site enables you to explore HPE Product Solutions to meet your business needs, includes a full list of Integrations between HPE Products, as well as a listing of ITIL Processes. The URL for this Web site is **http://h20230.www2.hp.com/sc/solutions/index.jsp**

About this PDF Version of Online Help

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

Contents

IBM WebSphere

This section includes the following topics:

Workflow type	Workflow name
Provisioning	"Provision WebSphere and Custom Node" on page 22
	"Provision WebSphere Custom Node Profile From Existing Install" on the next page
	" Provision WebSphere and Deployment Manager" on page 40
	"Provision WebSphere and Stand-Alone" on page 58
	"Provision WebSphere Stand-Alone Profile From Existing Install" on page 76
	"Provision IBM HTTP Server and Plug-in" on page 91
	"Provision WebSphere 7 and Custom Node" on page 112
	"Provision WebSphere 7 and Deployment Manager" on page 128
	"Provision WebSphere 7 StandAlone Profile" on page 143
	"Provision IBM HTTP Server 7 and Plug-In" on page 157
	"Create Custom Node from Existing WebSphere 7 Install" on page 186
	"Create StandAlone from Existing WebSphere 7 Install" on page 174
Patching	"WebSpehere 8 - Patch Network Cell" on page 288
Configuring	"Create and Configure WebSphere Data Sources" on page 200
	"Create and Configure WebSphere Web Server Definitions" on page 223
	"Configure WebSphere Cluster and Cluster Members" on page 238
Release Management	"WebSphere - Code Release" on page 258
	"WebSphere - Code Release on Cluster" on page 273

Provision WebSphere Custom Node Profile From Existing Install

Use this workflow to create a custom profile on an existing WebSphere 8.0 or 8.5.x installation.

A custom profile initially contains an empty node with no servers. The workflow can add (federate) the server to the pertinent cell when the profile is created, or you can add it later yourself.

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

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

Prerequisites for this Workflow

Be sure that the following prerequisites are satisfied before you run the WebSphere 8.0 or 8.5.x workflow:

1. This workflow requires unchallenged `sudo` access to a user (typically root) who can access all required files and directories.
2. Per the IBM WebSphere 8 documentation, the following system libraries are required before provisioning IBM WebSphere Application Server Network Deployment version 8.0 or 8.5.x on 64-bit and 32-bit Red Hat Linux targets:

Platform	Required Library
64-bit Red Hat Enterprise Linux version 5	compat-libstdc++-33-3.2.3-61 compat-db-4.2.52-5.1 gtk2-2.10.4-29.el5 gtk2-engines-2.8.0-3.el5 ksh-20080202-14 libXp-1.0.0-8 libXmu-1.0.2-5 libXtst-1.0.1-3.1 pam-0.99.6.2-3.26.el5 elfutils-0.125-3.el5 elfutils-libs-0.125-3.el5 libXft-2.1.10-1.1 libstdc++-4.1.2-48 If the target server supports both 32-bit and 64-bit applications then both the 32-bit and 64-bit versions of the following libraries are required: compat-libstdc++-33-3.2.3-61 compat-db-4.2.52-5.1 gtk2-2.18.9-4 gtk2-engines-2.18.4-5 libstdc++-4.1.2-48 libXft-2.1.10-1.1 libXp-1.0.0-8 libXmu-1.0.2-5 libXtst-1.0.1-3.1 pam-0.99.6.2-3.26.el5
64-bit Red Hat Enterprise Linux version 6	compat-libstdc++-33-3.2.3-69 compat-db-4.6.21-15 ksh-20100621-2 gtk2-2.18.9-4

Platform	Required Library
	gtk2-engines-2.18.4-5 libXp-1.0.0-15.1 libXmu-1.0.5-1 libXtst-1.0.99.2-3 pam-1.1.1-4 elfutils-0.148-1 elfutils-libs-0.148-1 libXft-2.1.13-4.1 libstdc++-4.4.4-13 If the target server supports both 32-bit and 64-bit applications then both the 32-bit and 64-bit versions of the following libraries are required: compat-libstdc++-33-3.2.3-69 compat-db-4.6.21-15 libstdc++-4.4.4-13 libXp-1.0.0-15.1 libXmu-1.0.5-1 libXtst-1.0.99.2-3 pam-1.1.1-4 libXft-2.1.13-4.1 gtk2-2.18.9-4 gtk2-engines-2.18.4-5

Make sure that these libraries exist on each target server before running this workflow. If newer versions of these libraries are available, you can install the newer versions.

3. This workflow will install WebSphere Application Server as root because of the following IBM documented limitations:
   - Creation of a Linux service for WebSphere Application Server
   - Native registration with the operating system
   - Port conflicts that may occur with other installations of WebSphere Application Server that are not registered with the operating system

   If there is a need to run as a non-root user after installation, you can run a recursive `chown` under the installation root and set owner permissions accordingly.

For more information about prerequisites for WebSphere 8, refer to the WebSphere 8 Product Documentation.

How this Workflow Works

This topic contains the following information about the "Provision WebSphere Custom Node Profile From Existing Install" workflow:

Overview

This workflow creates a Custom Node profile on an existing WebSphere 8.0 or 8.5.x installation.

See the following topics for detailed information:

Validation Checks Performed

Steps in this Workflow

Process Flow

Validation Checks Performed

Most of the validation centers on special characters and spaces in the parameters. There are also validation checks that happen at the operating system level, including file system space checks and RPM checks (on Red Hat Linux platforms only).

The workflow first performs the following parameter checks:

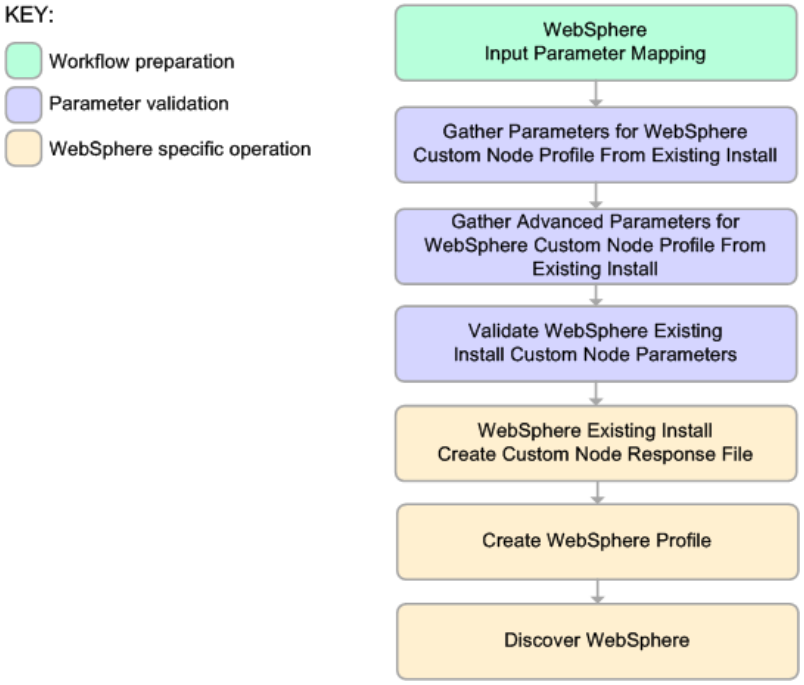
1. Required parameters have values specified.
2. WebSphere specific names do not contain the following characters: / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }
3. Parameters do not contain illegal characters for the parameter type.
4. Flag parameters are set to true or false.
5. Integer parameters are set to appropriate integer values.
6. Mutually dependent parameters are specified appropriately as a set.
7. Parameters are set to one of the values if the parameter has a list of valid values.
8. License Acceptance is true (for workflows that input the License Acceptance parameter).
9. All specified file names are legal file names.
10. All specified locations are legal path names. If they do not exist they will be created.

Note: For more information about valid parameter values, see "Parameters for Provision WebSphere Custom Node Profile From Existing Install ".

The workflow then checks to make sure that all required libraries are present on the target machine (see "Prerequisites for this Workflow").

Steps Executed

The Provision WebSphere Stand-Alone Profile From Existing Install workflow includes the following steps. Each step must complete successfully before the next step can start. If a step fails, the workflow reports a failure, and all subsequent steps are skipped.



Process Flow

This workflow performs the following tasks:

1. Creates the call wrapper and determines the target server platform type.
2. Gathers and validates the parameters needed to create a Custom Node profile (see "Validation Checks Performed " on the previous page).
3. Creates a new response file for the purpose of creating a Custom Node profile on top of the existing WebSphere 8.0 or 8.5.x installation.
4. Creates a Custom Node profile on top of the WebSphere 8.0 or 8.5.x installation.
5. Federates into the Deployment Manager.
6. Discovers any WebSphere 8.0 or 8.5.x cells, clusters, and managed servers associated with the Profile Root that you specify. If these items are found, they are added to the HPE DMA environment.

How to Run this Workflow

The following instructions show you how to customize and run the "Provision WebSphere Custom Node Profile From Existing Install" workflow in your environment.

The workflow provides default values for some parameters. These default values are usually sufficient for a "typical" installation. You can override the defaults by specifying parameter values in the deployment. You can also expose additional parameters in the workflow, if necessary, to accomplish more advanced scenarios. Any parameters not explicitly specified in the deployment will have the default values listed in "Parameters for Provision WebSphere Custom Node Profile From Existing Install ".

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

To use the Provision WebSphere Stand-Alone Profile From Existing Install workflow:

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

   Parameters Defined in this Step: Gather Parameters for WebSphere Existing Install Stand Alone

Parameter Name	Default Value	Required	Description
Cell Name	no default	required	Unique cell name that does not contain any of the following special characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }. If you plan to federate into an existing cell later, make sure that this name is not the same as the existing cell name.
Dmgr Admin Password	no default	optional	Administrative user password for the Deployment Manager. When Enable Security is set to true, this parameter must contain a string that does not begin with a dash(-) or contain a space( ).
Dmgr Admin User	no default	optional	Deployment Manager administrative user. When Enable Security is set to true, this parameter must contain a string that does not begin with a dash(-), a period(.), or a space( ). It cannot contain any of the following characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }.
Dmgr HostName	no default	optional	Host name or IP address of the machine where the Deployment Manager is running. Specify this parameter and the Dmgr Port parameter to federate the new custom node as it is created. If you do not specify a value for this parameter, the new custom node is not federated (you must federate it later). Required if Federate Later is set to false.
Dmgr Port	no default	optional	The SOAP port on which the Deployment Manager is listening. Specify this parameter and the Dmgr Host Name parameter to federate the new custom node as it is created. If you do not specify a value for this parameter, the new custom node is not

Parameters Defined in this Step: Gather Parameters for WebSphere Existing Install Stand Alone , continued

Parameter Name	Default Value	Required	Description
			federated (you must federate it later). Required if Federate Later is set to false.
Enable Security	no default	required	Enables administrative security on the Deployment Manager. Must be set to either true or false. If Enable Security is true, the Dmgr Admin User and Dmgr Admin Password parameters must have values.
Node Name	no default	required	Unique node name that cannot contain any of the following special characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }. If you plan to federate into an existing cell later, make sure that the name is unique within that cell.
Profile Name	no default	required	A unique profile name. It cannot begin with a period (.) and cannot contain any of the following special characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }.
Web Service Password	no default	required	Password for the discovery web service API.
Web Service User	no default	required	User capable of modifying the managed environment through the discovery web service API.
WebSphere Install Location	no default	required	Fully qualified path where WebSphere will be installed.
Windows Administrator Password	no default	required	The Windows Administrator password. Required for Windows.
Windows Administrator User	no default	required	This is the Windows Administrator user. Required for Windows.

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

See "Parameters for Provision WebSphere Custom Node Profile From Existing Install " for detailed descriptions of all input parameters for this workflow, including default values.

Tip: To avoid having to re-enter passwords whenever they change, you can create a policy to provide them to the workflow.

3. In the workflow editor, expose any additional parameters that you need. You will specify values for those parameters when you create the deployment.

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

To verify the results:

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

Be sure to also perform the following steps:

1. After the workflow has completed, run the following command to check the version of WebSphere Application Server that was installed:

   WAS_ROOT/bin/versionInfo.sh

   Here, *WAS_ROOT* is the directory where WebSphere 8.0 or 8.5.x is installed. This is the path that you specified in the WebSphere Install Location parameter.
2. Validate that the profile has been created and is running by doing the following:
   a. View the *WAS_ROOT*/profiles/*PROFILE_NAME*/logs/AboutThisProfile.txt file. This file is created after the creation of the profile and contains specific information about the profile.

      Here, *PROFILE_NAME* is the name of the profile that you just created. This is the name that you specified in the Profile Name parameter.

   b. Change to the *WAS_ROOT*/profiles/*PROFILE_NAME*/logs/*CELL_NAME* directory, and tail the SystemOut.log file. Look for the following line:

      Server *CELL_NAME* open for e-business

      Here, *CELL_NAME* is the name of the WebSphere 8.0 or 8.5.x cell to which this profile pertains. This is the name that you specified in the Cell Name parameter.

Sample Scenario

This topic shows you typical parameter values used for the "Provision WebSphere Custom Node Profile From Existing Install" workflow.

Tip: To avoid having to re-enter passwords whenever they change, you can create a policy to provide them to the workflow.

Custom Node Profiles on Existing Install – Parameter Value Examples

Parameter Name	Example Value	Description
Cell Name	Dev NodeCell	Unique cell name that does not contain any of the following special characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }. If you plan to federate into an existing cell later, make sure that this name is not the same as the existing cell name.
Dmgr Admin Password	wasPassWord	Administrative user password for the Deployment Manager. When Enable Security is set to true, this parameter must contain a string that does not begin with a dash(-) or contain a space( ).
Dmgr Admin User	wasadmin	Deployment Manager administrative user. When Enable Security is set to true, this parameter must contain a string that does not begin with a dash(-), a period(.), or a space( ). It cannot contain any of the following characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }.
Dmgr HostName	testserver.mycompany.com	Host name or IP address of the machine where the Deployment Manager is running. Specify this parameter and the Dmgr Port parameter to federate the new custom node as it is created. If you do not specify a value for this parameter, the new custom node is not federated (you must federate it later). Required if Federate Later is set to false.
Dmgr Port	8879	The SOAP port on which the Deployment Manager is listening. Specify this parameter and the Dmgr Host Name parameter to federate the new custom node as it is created. If you do not specify a value for this parameter, the new custom node is not federated (you must federate it later). Required if Federate Later is set to false.
Enable Security	true	Enables administrative security on the Deployment Manager. Must be set to either true or false. If Enable Security is true, the Dmgr Admin User and Dmgr Admin Password parameters must have values.
Node Name	DevNode1	Unique node name that cannot contain any of the following special characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }. If you plan to federate into an existing cell later, make sure that the name is unique within that cell.

Custom Node Profiles on Existing Install – Parameter Value Examples , continued

Parameter Name	Example Value	Description
Profile Name	DevNode1	A unique profile name. It cannot begin with a period (.) and cannot contain any of the following special characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }.
Web Service Password	myWebSvcPwd	Password for the discovery web service API.
Web Service User	JohnDoe	User capable of modifying the managed environment through the discovery web service API.
WebSphere Install Location	/opt/IBM/ WebSphere/AppServer	Fully qualified path where WebSphere will be installed.

Parameters for Provision WebSphere Custom Node Profile From Existing Install

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

Input Parameters Defined in this Step: Gather Parameters for WebSphere Existing Install Stand Alone

Parameter Name	Default Value	Required	Description
Call Wrapper	see description	required	Command that will execute this step (or subsequent steps) as a specific user. Defaults are: UNIX targets: `/opt/hp/dma/client/jython.sh` running as root Windows targets: `jython` running as Administrator
Cell Name	no default	required	Unique cell name that does not contain any of the following special characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }. If you plan to federate into an existing cell later, make sure that this name is not the same as the existing cell name.
Dmgr Admin Password	no default	optional	Administrative user password for the Deployment Manager. When Enable Security is set to true, this parameter must contain a string that does not begin with a dash(-) or contain a space( ).
Dmgr Admin User	no default	optional	Deployment Manager administrative user. When Enable Security is set to true, this parameter must contain a string that does not begin with a dash(-), a period(.), or a space( ). It cannot contain any of the following characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }.
Dmgr HostName	no default	optional	Host name or IP address of the machine where the Deployment Manager is running. Specify this parameter and the Dmgr Port parameter to federate the new custom node as it is created. If you do not specify a value for this parameter, the new custom node is not federated (you must federate it later). Required if Federate Later is set to false.
Dmgr Port	no default	optional	The SOAP port on which the Deployment Manager is listening. Specify this parameter and the Dmgr Host Name parameter to federate the new custom node as it is created. If you do not specify a value for this parameter, the new custom node is not federated (you must federate it later). Required if Federate Later is set to false.
Enable Security	no default	required	Enables administrative security on the Deployment Manager. Must be set to either true or false. If Enable Security is true, the Dmgr Admin User and Dmgr Admin Password parameters

Input Parameters Defined in this Step: Gather Parameters for WebSphere Existing Install Stand Alone , continued

Parameter Name	Default Value	Required	Description
			must have values.
Host Name	Server.name	required	Hostname or IP address of the target machine.
Node Name	no default	required	Unique node name that cannot contain any of the following special characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }. If you plan to federate into an existing cell later, make sure that the name is unique within that cell.
Profile Name	no default	required	A unique profile name. It cannot begin with a period (.) and cannot contain any of the following special characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }.
Web Service Password	no default	required	Password for the discovery web service API.
Web Service User	no default	required	User capable of modifying the managed environment through the discovery web service API.
WebSphere Install Location	no default	required	Fully qualified path where WebSphere will be installed.
Windows Administrator Password	no default	required	The Windows Administrator password. Required for Windows.
Windows Administrator User	no default	required	This is the Windows Administrator user. Required for Windows.

Additional Input Parameters Defined in this Step: Gather Advanced Parameters for WebSphere Existing Install Stand Alone

Parameter Name	Default Value	Required	Description
Keystore Password	no default	optional	Sets the password for all keystore files created during profile creation. This includes keystore files for both the default personal certificate and the root signing certificate.
Personal CertDN	no default	optional	Distinguished name of the personal certificate. For example: CN=dmalab-example.com,OU=WAS7LabCell, OU=WAS7LabDmgrManager,O=IBM,C=US The DN string cannot contain spaces. If you do not specify the DN, the WebSphere Application Server installer will create one.

Additional Input Parameters Defined in this Step: Gather Advanced Parameters for WebSphere Existing Install Stand Alone, continued

Parameter Name	Default Value	Required	Description
Personal CertValidity Period	1	optional	Amount of time in years that the personal certificate is valid. Default is one year.
Ports File	no default	optional	Fully qualified path to a file that defines port settings for the new profile. This file must contain key=value pairs that specify a service name and a port number (for example: WC_adminhost=9060). This option should be used with the Validate Ports option.
Profile Response File	no default	optional	Fully qualified path where the response file that this workflow creates will be located. This file will then be used to drive the installation.
Response File	no default	optional	Fully qualified path where the response file that this workflow creates will be located. This file will then be used to drive the installation and profile creation.
Signing CertDN	no default	optional	Distinguished name of the signing certificate. For example: CN=dmalab-example.com, OU=Root Certificate, OU=WAS7TestLabCell, OU=WAS7LabNode1, O=IBM, C=US The DN string cannot contain spaces. If you do not specify the DN, the WebSphere Application Server installer will create one.
Signing CertValidity Period	15	optional	Amount of time in years that the root certificate is valid. Default is 15 years.

Provision WebSphere and Custom Node

Use this workflow to install the WebSphere 8.0 or 8.5.x Base core binaries and, optionally, create a custom profile.

A custom profile initially contains an empty node with no servers. The workflow can add (federate) the server to the pertinent cell when the profile is created, or you can add it later yourself.

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

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

Note: The documentation for this workflow contains steps that are referred to by their base names. The names in the HPE DMA user interface may have a version appended, for example, v2.

Prerequisites for this Workflow

Be sure that the following prerequisites are satisfied before you run the Provision WebSphere and Custom Node workflow:

1. This workflow requires unchallenged `sudo` access to a user (typically root) who can access all required files and directories.
2. Per the IBM WebSphere 8 documentation, the following system libraries are required before provisioning WebSphere 8.0 or 8.5.x on 64-bit and 32-bit Red Hat Linux targets:

Platform	Required Library
64-bit Red Hat Enterprise Linux version 5	compat-libstdc++-33-3.2.3-61 compat-db-4.2.52-5.1 gtk2-2.10.4-29.el5 gtk2-engines-2.8.0-3.el5 ksh-20080202-14 libXp-1.0.0-8 libXmu-1.0.2-5 libXtst-1.0.1-3.1 pam-0.99.6.2-3.26.el5 elfutils-0.125-3.el5 elfutils-libs-0.125-3.el5 libXft-2.1.10-1.1 libstdc++-4.1.2-48 If the target server supports both 32-bit and 64-bit applications then both the 32-bit and 64-bit versions of the following libraries are required: compat-libstdc++-33-3.2.3-61 compat-db-4.2.52-5.1 gtk2-2.18.9-4 gtk2-engines-2.18.4-5 libstdc++-4.1.2-48 libXft-2.1.10-1.1 libXp-1.0.0-8 libXmu-1.0.2-5 libXtst-1.0.1-3.1 pam-0.99.6.2-3.26.el5
64-bit Red Hat Enterprise Linux version 6	compat-libstdc++-33-3.2.3-69 compat-db-4.6.21-15 ksh-20100621-2 gtk2-2.18.9-4 gtk2-engines-2.18.4-5 libXp-1.0.0-15.1 libXmu-1.0.5-1 libXtst-1.0.99.2-3

Platform	Required Library
	pam-1.1.1-4 elfutils-0.148-1 elfutils-libs-0.148-1 libXft-2.1.13-4.1 libstdc++-4.4.4-13 If the target server supports both 32-bit and 64-bit applications then both the 32-bit and 64-bit versions of the following libraries are required: compat-libstdc++-33-3.2.3-69 compat-db-4.6.21-15 libstdc++-4.4.4-13 libXp-1.0.0-15.1 libXmu-1.0.5-1 libXtst-1.0.99.2-3 pam-1.1.1-4 libXft-2.1.13-4.1 gtk2-2.18.9-4 gtk2-engines-2.18.4-5

Make sure that these libraries exist on each target server before running this workflow. If newer versions of these libraries are available, you can install the newer versions.

3. This workflow will install WebSphere Application Server as root because of the following IBM documented limitations:
   - Creation of a Linux service for WebSphere Application Server
   - Native registration with the operating system
   - Port conflicts that may occur with other installations of WebSphere Application Server that are not registered with the operating system

   If there is a need to run as a non-root user after installation, you can run a recursive `chown` under the installation root and set owner permissions accordingly.

For more information about prerequisites for WebSphere 8, refer to the WebSphere 8 Product Documentation.

How this Workflow Works

This topic contains the following information about the "Provision WebSphere and Custom Node" workflow:

Overview

This workflow does the following three things in the order shown:

1. Installs the IBM Install Manager
2. Installs WebSphere Network Deployment version 8.0 or 8.5.x
3. Creates a Custom Node profile

The workflow checks to see if the WebSphere 8.0 or 8.5.x binary archive files exist on the target machine. If they do not, the files are downloaded from the software repository.

See the following topics for detailed information:

Validation Checks Performed

Steps in this Workflow

Process Flow

Note: This workflow has been updated to account for the significant changes in the way that WebSphere 8 are installed.

Validation Checks Performed

Most of the validation centers on special characters and spaces in the parameters. There are also validation checks that happen at the operating system level, including file system space checks and RPM checks (on Red Hat Linux platforms only).

The workflow first performs the following parameter checks:

1. Required parameters have values specified.
2. WebSphere specific names do not contain the following characters: / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }
3. Parameters do not contain illegal characters for the parameter type.
4. Flag parameters are set to true or false.
5. Integer parameters are set to appropriate integer values.
6. Mutually dependent parameters are specified appropriately as a set.
7. Parameters are set to one of the values if the parameter has a list of valid values.
8. License Acceptance is true (for workflows that input the License Acceptance parameter).
9. All specified file names are legal file names.
10. All specified locations are legal path names. If they do not exist they will be created.

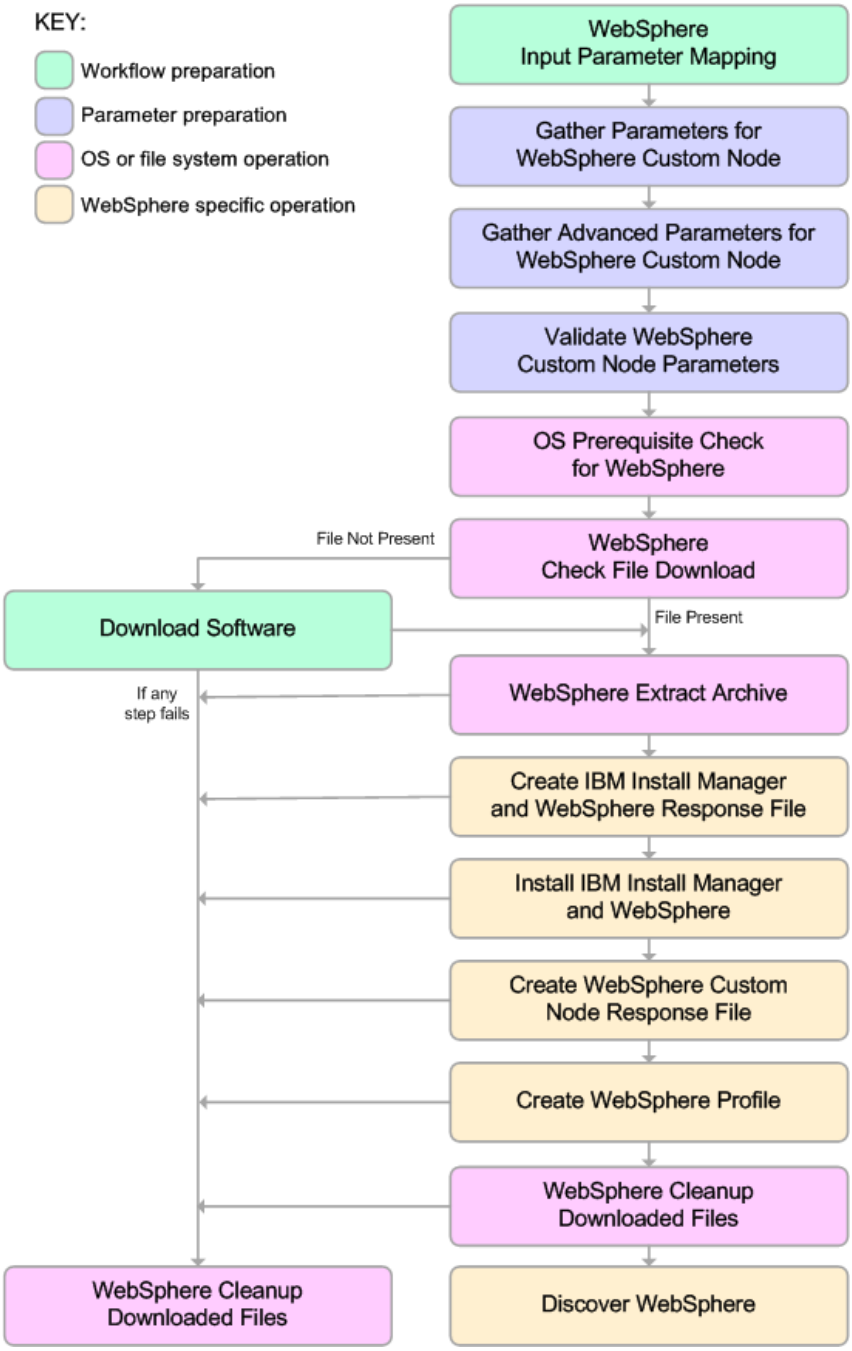
Note: For more information about valid parameter values, see "Parameters for Provision WebSphere and Custom Node".

The workflow then performs the following operating system checks on the target machine:

1. All required libraries are present (see "Prerequisites for this Workflow").
2. Sufficient disk space is available to install WebSphere 8.0 or 8.5.x.
3. Sufficient disk space is available to extract the binary files from the compressed archive.

Steps Executed

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



Process Flow

This workflow performs the following tasks:

1. Creates the call wrapper and determines the target server platform type.
2. Gathers and validates the parameters needed to install Provision WebSphere and Custom Node and create a Custom Node profile (see "Validation Checks Performed " on page 26).
3. Checks the following:
   a. Documented library requirements for WebSphere 8 (see the "Prerequisites for this Workflow").
   b. File system space requirements where WebSphere 8.0 or 8.5.x will be installed.
   c. Temporary space requirements where the compressed software will be extracted before it is installed.
4. Determines whether the WebSphere 8.0 or 8.5.x binary archive is present on the target machine. If the archive is not present, the workflow downloads it from the software repository.
5. Extracts the WebSphere 8.0 or 8.5.x binary archive to the specified directory.
6. Creates a response file for the purpose of installing a new instance of WebSphere 8.0 or 8.5.x.
7. Installs the IBM Installation Manager and a new WebSphere 8.0 or 8.5.x instance on the target server.
8. Creates a new response file for the purpose of creating a Custom Node profile on top of the WebSphere 8.0 or 8.5.x installation.
9. Creates a custom profile on top of the WebSphere 8.0 or 8.5.x installation.
10. Cleans up any files that were downloaded—for either workflow success or failure.

    Note: The parameters Cleanup on Success and Cleanup on Failure are defaulted to True. If they are set to False, the downloaded files are not cleaned up.

11. Discovers any WebSphere 8.0 or 8.5.x cells, clusters, and managed servers associated with the Profile Root that you specify. If these items are found, they are added to the HPE DMA environment.

How to Run this Workflow

The following instructions show you how to customize and run the "Provision WebSphere and Custom Node" workflow in your environment.

The workflow provides default values for some parameters. These default values are usually sufficient for a "typical" installation. You can override the defaults by specifying parameter values in the deployment. You can also expose additional parameters in the workflow, if necessary, to accomplish more advanced scenarios. Any parameters not explicitly specified in the deployment will have the default values listed in "Parameters for Provision WebSphere and Custom Node".

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

To use the Provision WebSphere and Custom Node workflow:

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

   Parameters Defined in this Step: Gather Parameters for WebSphere Custom Node

Parameter Name	Default Value	Required	Description
Cell Name	no default	required	Unique cell name that does not contain any of the following special characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }. If you plan to federate into an existing cell later, make sure that this name is not the same as the existing cell name.
Dmgr Admin Password	no default	optional	Administrative user password for the Deployment Manager. When Enable Security is set to true, this parameter must contain a string that does not begin with a dash(-) or contain a space( ).
Dmgr Admin User	no default	optional	Deployment Manager administrative user. When Enable Security is set to true, this parameter must contain a string that does not begin with a dash(-), a period(.), or a space( ). It cannot contain any of the following characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }.
Dmgr HostName	no default	optional	Host name or IP address of the machine where the Deployment Manager is running. Specify this parameter and the Dmgr Port parameter to federate the new custom node as it is created. If you do not specify a value for this parameter, the new custom node is not federated (you must federate it later). Required if Federate Later is set to false.
Dmgr Port	no default	optional	The SOAP port on which the Deployment Manager is listening. Specify this parameter and the Dmgr Host Name parameter to federate the new custom node as it is created. If you do not specify a value for this parameter, the new custom node is not federated (you must federate it later). Required if

Parameters Defined in this Step: Gather Parameters for WebSphere Custom Node, continued

Parameter Name	Default Value	Required	Description
			Federate Later is set to false.
Enable Security	no default	required	Enables administrative security on the Deployment Manager. Must be set to either true or false. If Enable Security is true, the Dmgr Admin User and Dmgr Admin Password parameters must have values.
Federate Later	no default	required	If false, the new custom node will be federated by the workflow during profile creation; you must specify Dmgr HostName and Dmgr Port to do this. If true, you must federate it later manually by using the addNode command.
Install Manager Binary Download Location	`/opt/IBM/iim`	required	Fully qualified path to where the compressed Install Manager software package will be downloaded on the target machine. For example: `/opt/IBM/iim`
Install Manager Binary Files	no default	required	Name of the compressed Install Manager software package.
Install Manager Extract Location	no default	required	Fully qualified path where the compressed software will be extracted on the target machine. This location cannot be the same as WebSphere Extract Location.
Install Manager Install Location	no default	required	Fully qualified path where Install Manager will be installed. For example: `/opt/IBM/InstallManager`
License Acceptance	false	required	Acknowledges that the end user agrees to the IBM International Program License Agreement. This is set to false by default and must be set to true in order for the installation to continue.
Node Name	no default	required	Unique node name that cannot contain any of the following special characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }. If you plan to federate into an existing cell later, make sure that the name is unique within that cell.
Profile Name	no default	required	A unique profile name. It cannot begin with a period (.) and cannot contain any of the following special characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }.
Web Service	no default	required	Password for the discovery web service API.

Parameters Defined in this Step: Gather Parameters for WebSphere Custom Node, continued

Parameter Name	Default Value	Required	Description
Password			
Web Service User	no default	required	User capable of modifying the managed environment through the discovery web service API.
WebSphere Binary Download Location	`/opt/IBM/WAS`	required	Fully qualified path to the compressed WebSphere software package on the target machine.
WebSphere Binary Files	no default	required	Comma separated list of file names of the compressed WebSphere software packages.
WebSphere Extract Location	no default	required	Fully qualified path where the compressed software will be extracted on the target machine. This location cannot be the same as Install Manager Extract Location.
WebSphere Install Location	no default	required	Fully qualified path where WebSphere will be installed.
Windows Administrator Password	no default	required	The Windows Administrator password. Required for Windows.
Windows Administrator User	no default	required	This is the Windows Administrator user. Required for Windows.

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

See "Parameters for Provision WebSphere and Custom Node" for detailed descriptions of all input parameters for this workflow, including default values.

Tip: To avoid having to re-enter passwords whenever they change, you can create a policy to provide them to the workflow

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

9. Run the workflow using this deployment.

To verify the results:

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

Be sure to also perform the following steps:

1. After the workflow has completed, run the following command to check the version of WebSphere Application Server that was installed:

   WAS_ROOT/bin/versionInfo.sh

   Here, *WAS_ROOT* is the directory where WebSphere 8.0 or 8.5.x is installed. This is the path that you specified in the WebSphere Install Location parameter.
2. Validate that the profile has been created and is running by doing the following:
   a. View the *WAS_ROOT*/profiles/*PROFILE_NAME*/logs/AboutThisProfile.txt file. This file is created after the creation of the profile and contains specific information about the profile.

      Here, *PROFILE_NAME* is the name of the profile that you just created. This is the name that you specified in the Profile Name parameter.

   b. Change to the *WAS_ROOT*/profiles/*PROFILE_NAME*/logs/*CELL_NAME* directory, and tail the SystemOut.log file. Look for the following line:

      Server *CELL_NAME* open for e-business

      Here, *CELL_NAME* is the name of the WebSphere 8.0 or 8.5.x cell to which this profile pertains. This is the name that you specified in the Cell Name parameter.

Sample Scenario

This topic shows you typical parameter values used for the "Provision WebSphere and Custom Node" workflow.

Tip: To avoid having to re-enter passwords whenever they change, you can create a policy to provide them to the workflow.

New Install with Custom Node Profile – Parameter Value Examples

Parameter Name	Example Value	Description
Cell Name	Dev NodeCell	Unique cell name that does not contain any of the following special characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }. If you plan to federate into an existing cell later, make sure that this name is not the same as the existing cell name.
Dmgr Admin Password	wasPassWord	Administrative user password for the Deployment Manager. When Enable Security is set to true, this parameter must contain a string that does not begin with a dash(-) or contain a space( ).
Dmgr Admin User	wasadmin	Deployment Manager administrative user. When Enable Security is set to true, this parameter must contain a string that does not begin with a dash(-), a period(.), or a space( ). It cannot contain any of the following characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }.
Dmgr HostName		Host name or IP address of the machine where the Deployment Manager is running. Specify this parameter and the Dmgr Port parameter to federate the new custom node as it is created. If you do not specify a value for this parameter, the new custom node is not federated (you must federate it later). Required if Federate Later is set to false.
Dmgr Port		The SOAP port on which the Deployment Manager is listening. Specify this parameter and the Dmgr Host Name parameter to federate the new custom node as it is created. If you do not specify a value for this parameter, the new custom node is not federated (you must federate it later). Required if Federate Later is set to false.
Enable Security	true	Enables administrative security on the Deployment Manager. Must be set to either true or false. If Enable Security is true, the Dmgr Admin User and Dmgr Admin Password parameters must have values.
Federate Later	true	If false, the new custom node will be federated by the workflow during profile creation; you must specify Dmgr HostName and Dmgr Port to do this. If true, you must federate it later manually by using the addNode command.
Install Manager	/opt/IBM/iim	Fully qualified path to where the compressed Install Manager software package will be downloaded on the target machine. For

New Install with Custom Node Profile – Parameter Value Examples, continued

Parameter Name	Example Value	Description
Binary Download Location		example: `/opt/IBM/iim`
Install Manager Binary Files	IBM_Install_Manager_Linux.zip	Name of the compressed Install Manager software package.
Install Manager Extract Location	/opt/IBM/iim	Fully qualified path where the compressed software will be extracted on the target machine. This location cannot be the same as WebSphere Extract Location.
Install Manager Install Location	/opt/IBM/installManager	Fully qualified path where Install Manager will be installed. For example: `/opt/IBM/InstallManager`
License Acceptance	true	Acknowledges that the end user agrees to the IBM International Program License Agreement. This is set to false by default and must be set to true in order for the installation to continue.
Node Name	DevNode	Unique node name that cannot contain any of the following special characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }. If you plan to federate into an existing cell later, make sure that the name is unique within that cell.
Profile Name	DevNode	A unique profile name. It cannot begin with a period (.) and cannot contain any of the following special characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }.
Web Service Password	myWebSvcPwd	Password for the discovery web service API.
Web Service User	JohnDoe	User capable of modifying the managed environment through the discovery web service API.
WebSphere Binary Download Location	/opt/IBM/was	Fully qualified path to the compressed WebSphere software package on the target machine.
WebSphere Binary Files	WAS_V8.0_disk1.zip, WAS_V8.0_disk2.zip	Comma separated list of file names of the compressed WebSphere software packages.
WebSphere Extract Location	/opt/IBM/was	Fully qualified path where the compressed software will be extracted on the target machine. This location cannot be the same as Install Manager Extract Location.

New Install with Custom Node Profile – Parameter Value Examples, continued

Parameter Name	Example Value	Description
WebSphere Install Location	/opt/IBM/ WebSphere/AppServer	Fully qualified path where WebSphere will be installed.

Parameters for Provision WebSphere and Custom Node

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

Input Parameters Defined in this Step: Gather Parameters for WebSphere Custom Node

Parameter Name	Default Value	Required	Description
Call Wrapper	see description	required	Command that will execute this step (or subsequent steps) as a specific user. Defaults are: UNIX targets: `/opt/hp/dma/client/jython.sh` running as root Windows targets: `jython` running as Administrator
Cell Name	no default	required	Unique cell name that does not contain any of the following special characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }. If you plan to federate into an existing cell later, make sure that this name is not the same as the existing cell name.
Dmgr Admin Password	no default	optional	Administrative user password for the Deployment Manager. When Enable Security is set to true, this parameter must contain a string that does not begin with a dash(-) or contain a space( ).
Dmgr Admin User	no default	optional	Deployment Manager administrative user. When Enable Security is set to true, this parameter must contain a string that does not begin with a dash(-), a period(.), or a space( ). It cannot contain any of the following characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }.
Dmgr HostName	no default	optional	Host name or IP address of the machine where the Deployment Manager is running. Specify this parameter and the Dmgr Port parameter to federate the new custom node as it is created. If you do not specify a value for this parameter, the new custom node is not federated (you must federate it later). Required if Federate Later is set to false.
Dmgr Port	no default	optional	The SOAP port on which the Deployment Manager is listening. Specify this parameter and the Dmgr Host Name parameter to federate the new custom node as it is created. If you do not specify a value for this parameter, the new custom node is not federated (you must federate it later). Required if Federate Later is set to false.
Enable Security	no default	required	Enables administrative security on the Deployment Manager. Must be set to either true or false. If Enable Security is true, the Dmgr Admin User and Dmgr Admin Password parameters must have values.

Input Parameters Defined in this Step: Gather Parameters for WebSphere Custom Node, continued

Parameter Name	Default Value	Required	Description
Federate Later	no default	required	If false, the new custom node will be federated by the workflow during profile creation; you must specify Dmgr HostName and Dmgr Port to do this. If true, you must federate it later manually by using the addNode command.
Host Name	Server.name	required	Hostname or IP address of the target machine.
Install Manager Binary Download Location	`/opt/IBM/iim`	required	Fully qualified path to where the compressed Install Manager software package will be downloaded on the target machine. For example: `/opt/IBM/iim`
Install Manager Binary Files	no default	required	Name of the compressed Install Manager software package.
Install Manager Extract Location	no default	required	Fully qualified path where the compressed software will be extracted on the target machine. This location cannot be the same as WebSphere Extract Location.
Install Manager Install Location	no default	required	Fully qualified path where Install Manager will be installed. For example: `/opt/IBM/InstallManager`
License Acceptance	false	required	Acknowledges that the end user agrees to the IBM International Program License Agreement. This is set to false by default and must be set to true in order for the installation to continue.
Node Name	no default	required	Unique node name that cannot contain any of the following special characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }. If you plan to federate into an existing cell later, make sure that the name is unique within that cell.
Profile Name	no default	required	A unique profile name. It cannot begin with a period (.) and cannot contain any of the following special characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }.
Web Service Password	no default	required	Password for the discovery web service API.
Web Service User	no default	required	User capable of modifying the managed environment through the discovery web service API.
WebSphere Binary	`/opt/IBM/WAS`	required	Fully qualified path to the compressed WebSphere software package on the target machine.

Input Parameters Defined in this Step: Gather Parameters for WebSphere Custom Node, continued

Parameter Name	Default Value	Required	Description
Download Location			
WebSphere Binary Files	no default	required	Comma separated list of file names of the compressed WebSphere software packages.
WebSphere Extract Location	no default	required	Fully qualified path where the compressed software will be extracted on the target machine. This location cannot be the same as Install Manager Extract Location.
WebSphere Install Location	no default	required	Fully qualified path where WebSphere will be installed.
Windows Administrator Password	no default	required	The Windows Administrator password. Required for Windows.
Windows Administrator User	no default	required	This is the Windows Administrator user. Required for Windows.

Additional Input Parameters Defined in this Step: Gather Advanced Parameters for WebSphere Custom Node

Parameter Name	Default Value	Required	Description
Cleanup on Failure	True	optional	Indicates whether to remove downloaded and extracted files and to clean up the installation directory in the event of workflow failure. Valid values are True and False. The default is True, which will clean up on failure.
Cleanup on Success	True	optional	Indicates whether to remove downloaded and extracted files and to clean up the installation directory in the event of workflow success. Valid values are True and False. The default is True, which will clean up on success.
Keystore Password	no default	optional	Sets the password for all keystore files created during profile creation. This includes keystore files for both the default personal certificate and the root signing certificate.
Personal CertDN	no default	optional	Distinguished name of the personal certificate. For example: CN=dmalab-example.com,OU=WAS7LabCell, OU=WAS7LabDmgrManager,O=IBM,C=US The DN string cannot contain spaces. If you do not specify the DN, the WebSphere Application Server installer will create one.
Personal	1	optional	Amount of time in years that the personal certificate is valid. Default

Additional Input Parameters Defined in this Step: Gather Advanced Parameters for WebSphere Custom Node, continued

Parameter Name	Default Value	Required	Description
CertValidity Period			is one year.
Ports File	no default	optional	Fully qualified path to a file that defines port settings for the new profile. This file must contain key=value pairs that specify a service name and a port number (for example: WC_adminhost=9060). This option should be used with the Validate Ports option.
Profile Response File	no default	optional	Fully qualified path where the response file that this workflow creates will be located. This file will then be used to drive the installation.
Response File	no default	optional	Fully qualified path where the response file that this workflow creates will be located. This file will then be used to drive the installation and profile creation.
Signing CertDN	no default	optional	Distinguished name of the signing certificate. For example: CN=dmalab-example.com, OU=Root Certificate, OU=WAS7TestLabCell, OU=WAS7LabNode1, O=IBM, C=US The DN string cannot contain spaces. If you do not specify the DN, the WebSphere Application Server installer will create one.
Signing CertValidity Period	15	optional	Amount of time in years that the root certificate is valid. Default is 15 years.

Provision WebSphere and Deployment Manager

Use this workflow to install a new instance of the IBM WebSphere Application Server Network Deployment version 8.0 or 8.5.x and Installation Manager, and then create a deployment manager profile.

A deployment manager is the administration point for a cell that contains multiple application servers. This type of profile is appropriate for distributed application server environments.

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

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

Note: The documentation for this workflow contains steps that are referred to by their base names. The names in the HPE DMA user interface may have a version appended, for example, v2.

Prerequisites for this Workflow

Be sure that the following prerequisites are satisfied before you run the Provision WebSphere and Deployment Manager workflow:

1. This workflow requires unchallenged sudo access to a user (typically root) who can access all required files and directories.
2. Per the IBM WebSphere 8 documentation, the following system libraries are required before provisioning IBM WebSphere Application Server Network Deployment version 8.0 or 8.5.x on 64-bit and 32-bit Red Hat Linux targets:

Platform	Required Library
64-bit Red Hat Enterprise Linux version 5	compat-libstdc++-33-3.2.3-61 compat-db-4.2.52-5.1 gtk2-2.10.4-29.el5 gtk2-engines-2.8.0-3.el5 ksh-20080202-14 libXp-1.0.0-8 libXmu-1.0.2-5 libXtst-1.0.1-3.1 pam-0.99.6.2-3.26.el5 elfutils-0.125-3.el5 elfutils-libs-0.125-3.el5 libXft-2.1.10-1.1 libstdc++-4.1.2-48 If the target server supports both 32-bit and 64-bit applications then both the 32-bit and 64-bit versions of the following libraries are required: compat-libstdc++-33-3.2.3-61 compat-db-4.2.52-5.1 gtk2-2.18.9-4 gtk2-engines-2.18.4-5 libstdc++-4.1.2-48 libXft-2.1.10-1.1 libXp-1.0.0-8 libXmu-1.0.2-5 libXtst-1.0.1-3.1 pam-0.99.6.2-3.26.el5

Platform	Required Library
64-bit Red Hat Enterprise Linux version 6	compat-libstdc++-33-3.2.3-69 compat-db-4.6.21-15 ksh-20100621-2 gtk2-2.18.9-4 gtk2-engines-2.18.4-5 libXp-1.0.0-15.1 libXmu-1.0.5-1 libXtst-1.0.99.2-3 pam-1.1.1-4 elfutils-0.148-1 elfutils-libs-0.148-1 libXft-2.1.13-4.1 libstdc++-4.4.4-13 If the target server supports both 32-bit and 64-bit applications then both the 32-bit and 64-bit versions of the following libraries are required: compat-libstdc++-33-3.2.3-69 compat-db-4.6.21-15 libstdc++-4.4.4-13 libXp-1.0.0-15.1 libXmu-1.0.5-1 libXtst-1.0.99.2-3 pam-1.1.1-4 libXft-2.1.13-4.1 gtk2-2.18.9-4 gtk2-engines-2.18.4-5

Make sure that these libraries exist on each target server before running this workflow. If newer versions of these libraries are available, you can install the newer versions.

3. This workflow will install WebSphere Application Server as root because of the following IBM documented limitations:
   - Creation of a Linux service for WebSphere Application Server
   - Native registration with the operating system
   - Port conflicts that may occur with other installations of WebSphere Application Server that are not registered with the operating system

If there is a need to run as a non-root user after installation, you can run a recursive `chown` under the installation root and set owner permissions accordingly.

For more information about prerequisites for WebSphere 8, refer to the WebSphere 8 Product Documentation.

How this Workflow Works

This topic contains the following information about the " Provision WebSphere and Deployment Manager" workflow:

Overview

This workflow does the following three things in the order shown:

1. Installs the IBM Install Manager
2. Installs IBM WebSphere Application Server Network Deployment version 8.0 or 8.5.x
3. Creates a Deployment Manager profile

The workflow checks to see if the WebSphere 8.0 or 8.5.x binary archive files exist on the target machine. If they do not, the files are downloaded from the software repository.

See the following topics for detailed information:

Validation Checks Performed

Steps in this Workflow

Process Flow

Note: This workflow has been updated to account for the significant changes in the way that WebSphere 8 are installed.

Validation Checks Performed

Most of the validation centers on special characters and spaces in the parameters. There are also validation checks that happen at the operating system level, including file system space checks and RPM checks (on Red Hat Linux platforms only).

The workflow first performs the following parameter checks:

1. Required parameters have values specified.
2. WebSphere specific names do not contain the following characters: / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }
3. Parameters do not contain illegal characters for the parameter type.
4. Flag parameters are set to true or false.
5. Integer parameters are set to appropriate integer values.
6. Mutually dependent parameters are specified appropriately as a set.
7. Parameters are set to one of the values if the parameter has a list of valid values.
8. License Acceptance is true (for workflows that input the License Acceptance parameter).
9. All specified file names are legal file names.
10. All specified locations are legal path names. If they do not exist they will be created.

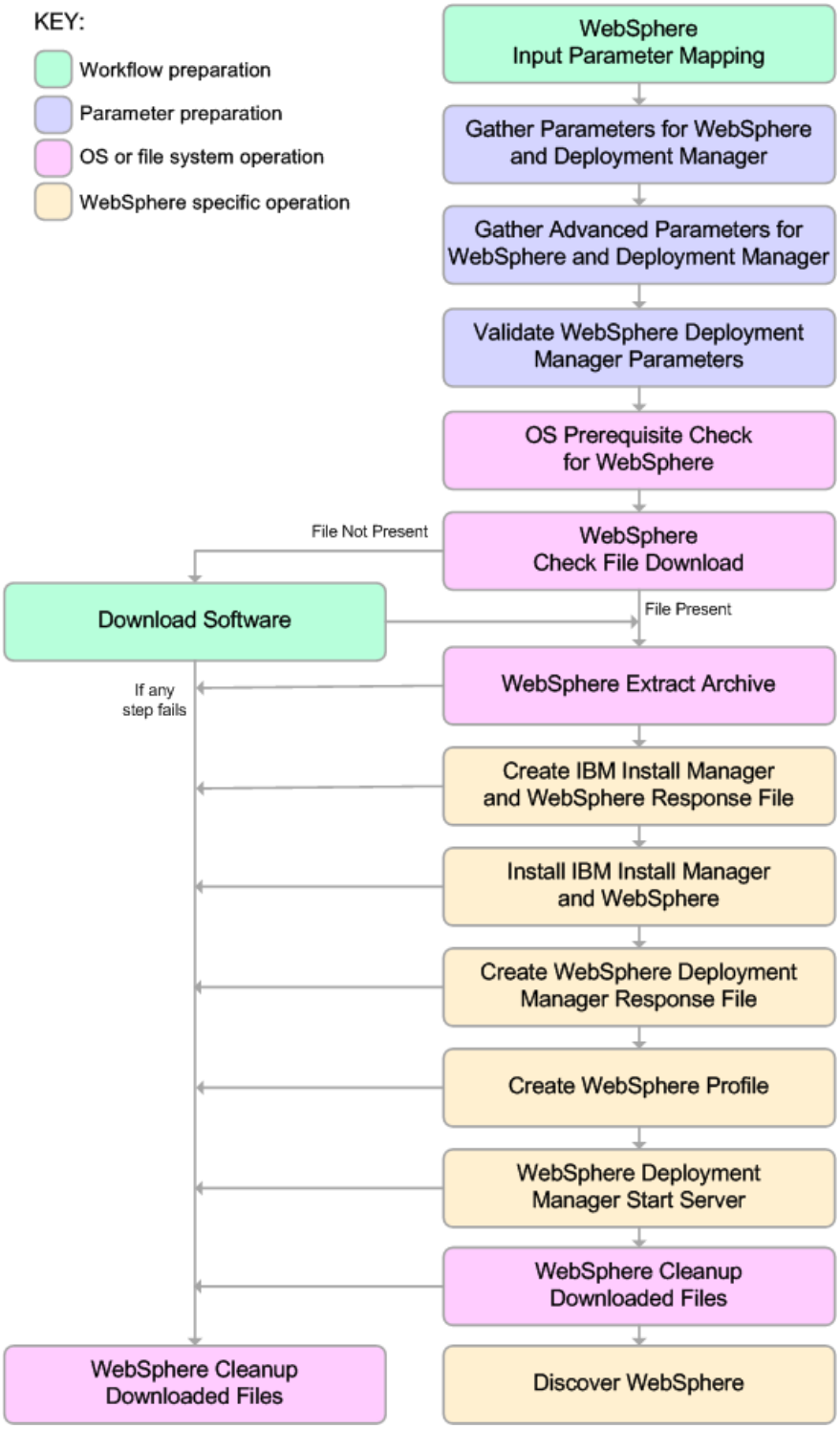
Note: For more information about valid parameter values, see "Parameters for Provision WebSphere and Deployment Manager".

The workflow then performs the following operating system checks on the target machine:

1. All required libraries are present (see "Prerequisites for this Workflow").
2. Sufficient disk space is available to install WebSphere 8.0 or 8.5.x.
3. Sufficient disk space is available to extract the binary files from the compressed archive.

Steps Executed

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



Process Flow

This workflow performs the following tasks:

1. Creates the call wrapper and determines the target server platform type.
2. Gathers and validates the parameters needed to install WebSphere 8.0 or 8.5.x and create a Deployment Manager profile (see "Validation Checks Performed " on page 45).
3. Checks the following:
   a. Documented library requirements for WebSphere 8 (see the "Prerequisites for this Workflow").
   b. File system space requirements where WebSphere 8.0 or 8.5.x will be installed.
   c. Temporary space requirements where the compressed software will be extracted before it is installed.
4. Determines whether the WebSphere 8.0 or 8.5.x binary archive is present on the target machine. If the archive is not present, the workflow downloads it from the software repository.
5. Extracts the WebSphere 8.0 or 8.5.x binary archive to the specified directory.
6. Creates a response file for the purpose of installing a new instance of WebSphere 8.0 or 8.5.x.
7. Installs the IBM Installation Manager and a new WebSphere 8.0 or 8.5.x instance on the target server.
8. Creates a new response file for the purpose of creating a Deployment Manager profile on top of the WebSphere 8.0 or 8.5.x installation.
9. Creates a Deployment Manager profile on top of the WebSphere 8.0 or 8.5.x installation.
10. Starts the new Deployment Manager WebSphere 8.0 or 8.5.x application server.
11. Cleans up any files that were downloaded—for either workflow success or failure.

    Note: The parameters Cleanup on Success and Cleanup on Failure are defaulted to True. If they are set to False, the downloaded files are not cleaned up.

12. Discovers any WebSphere 8.0 or 8.5.x cells, clusters, and managed servers associated with the Profile Root that you specify. If these items are found, they are added to the HPE DMA environment.

How to Run this Workflow

The following instructions show you how to customize and run the " Provision WebSphere and Deployment Manager" workflow in your environment.

The workflow provides default values for some parameters. These default values are usually sufficient for a "typical" installation. You can override the defaults by specifying parameter values in the deployment. You can also expose additional parameters in the workflow, if necessary, to accomplish more advanced scenarios. Any parameters not explicitly specified in the deployment will have the default values listed in "Parameters for Provision WebSphere and Deployment Manager".

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

To customize and run the Provision WebSphere and Deployment Manager workflow:

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

   Parameters Defined in this Step: Gather Parameters for WebSphere and Deployment Manager

Parameter Name	Default Value	Required	Description
Admin Password	no default	optional	When Enable Security is set to true, this parameter must contain a string that does not begin with a dash(-) or contain a space( ).
Admin User	no default	optional	When Enable Security is set to true, this parameter must contain a string that does not begin with a dash(-), a period(.), or a space( ). It cannot contain any of the following characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }.
Cell Name	no default	required	Unique cell name that does not contain any of the following special characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }. If you plan to federate into an existing cell later, make sure that this name is not the same as the existing cell name.
Enable Security	no default	required	Enables administrative security. Must be set to either true or false. If Enable Security is true, the Admin User and Admin Password parameters must have values.
Install Manager Binary Download Location	`/opt/IBM/iim`	required	Fully qualified path to where the compressed Install Manager software package will be downloaded on the target machine. For example: `/opt/IBM/iim`
Install Manager Binary Files	no default	required	Name of the compressed Install Manager software package.

Parameters Defined in this Step: Gather Parameters for WebSphere and Deployment Manager, continued

Parameter Name	Default Value	Required	Description
Install Manager Extract Location	no default	required	Fully qualified path where the compressed software will be extracted on the target machine. This location cannot be the same as WebSphere Extract Location.
Install Manager Install Location	no default	required	Fully qualified path where Install Manager will be installed. For example: `/opt/IBM/InstallManager`
License Acceptance	false	required	Acknowledges that the end user agrees to the IBM International Program License Agreement. This is set to false by default and must be set to true in order for the installation to continue.
Node Name	no default	required	Unique node name that cannot contain any of the following special characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }. If you plan to federate into an existing cell later, make sure that the name is unique within that cell.
Profile Name	no default	required	A unique profile name. It cannot begin with a period (.) and cannot contain any of the following special characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }.
Web Service Password	no default	required	Password for the discovery web service API.
Web Service User	no default	required	User capable of modifying the managed environment through the discovery web service API.
WebSphere Binary Download Location	`/opt/IBM/WAS`	required	Fully qualified path to the compressed WebSphere software package on the target machine.
WebSphere Binary Files	no default	required	Comma separated list of file names of the compressed WebSphere software packages.
WebSphere Extract Location	no default	required	Fully qualified path where the compressed software will be extracted on the target machine. This location cannot be the same as Install Manager Extract Location.
WebSphere Install Location	no default	required	Fully qualified path where WebSphere will be installed.
Windows	no default	required	The Windows Administrator password. Required for

Parameters Defined in this Step: Gather Parameters for WebSphere and Deployment Manager, continued

Parameter Name	Default Value	Required	Description
Administrator Password			Windows.
Windows Administrator User	no default	required	This is the Windows Administrator user. Required for Windows.

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

See "Parameters for Provision WebSphere and Deployment Manager" for detailed descriptions of all input parameters for this workflow, including default values.

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

To verify the results:

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

Be sure to also perform the following steps:

1. After the workflow has completed, run the following command to check the version of WebSphere Application Server that was installed:

   WAS_ROOT/bin/versionInfo.sh

   Here, *WAS_ROOT* is the directory where WebSphere 8.0 or 8.5.x is installed. This is the path that you specified in the WebSphere Install Location parameter.
2. Validate that the profile has been created and is running by doing the following:
   a. View the *WAS_ROOT*/profiles/*PROFILE_NAME*/logs/AboutThisProfile.txt file. This file is created after the creation of the profile and contains specific information about the profile.

      Here, *PROFILE_NAME* is the name of the profile that you just created. This is the name that you specified in the Profile Name parameter.

   b. Change to the *WAS_ROOT*/profiles/*PROFILE_NAME*/logs/*CELL_NAME* directory, and tail the SystemOut.log file. Look for the following line:

      Server *CELL_NAME* open for e-business

      Here, *CELL_NAME* is the name of the WebSphere 8.0 or 8.5.x cell to which this profile pertains. This is the name that you specified in the Cell Name parameter.

Sample Scenario

This topic shows you typical parameter values used for the " Provision WebSphere and Deployment Manager" workflow.

Tip: To avoid having to re-enter passwords whenever they change, you can create a policy to provide them to the workflow.

New Install with Deployment Manager – Parameter Value Examples

Parameter Name	Example Value	Description
Admin Password	wasPassWord	When Enable Security is set to true, this parameter must contain a string that does not begin with a dash(-) or contain a space( ).
Admin User	wasadmin	When Enable Security is set to true, this parameter must contain a string that does not begin with a dash(-), a period(.), or a space( ). It cannot contain any of the following characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }.
Cell Name	DevCell	Unique cell name that does not contain any of the following special characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }. If you plan to federate into an existing cell later, make sure that this name is not the same as the existing cell name.
Enable Security	true	Enables administrative security. Must be set to either true or false. If Enable Security is true, the Admin User and Admin Password parameters must have values.
Host Name	/opt/IBM/iim	Fully qualified path to where the compressed Install Manager software package will be downloaded on the target machine. For example: `/opt/IBM/iim`
Install Manager Binary Download Location	IBM_Install_Manager_Linux.zip	Name of the compressed Install Manager software package.
Install Manager Binary Files	/opt/IBM/iim	Fully qualified path where the compressed software will be extracted on the target machine. This location cannot be the same as Install Manager Extract Location.
Install Manager Extract Location	/opt/IBM/installManager	Fully qualified path where Install Manager will be installed. For example: `/opt/IBM/InstallManager`
Install Manager Install Location	true	Acknowledges that the end user agrees to the IBM International Program License Agreement. This is set to false by default and must be set to true in order for the installation to continue.

New Install with Deployment Manager – Parameter Value Examples, continued

Parameter Name	Example Value	Description
License Acceptance	DevManager	Unique node name that cannot contain any of the following special characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }. If you plan to federate into an existing cell later, make sure that the name is unique within that cell.
Node Name	DevDmgr	A unique profile name. It cannot begin with a period (.) and cannot contain any of the following special characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }.
Profile Name	myWebSvcPwd	Password for the discovery web service API.
Web Service Password	JohnDoe	User capable of modifying the managed environment through the discovery web service API.
Web Service User	/opt/IBM/was	Fully qualified path to the compressed WebSphere software package on the target machine.
WebSphere Binary Download Location	WAS_V8.0_disk1.zip, WAS_V8.0_disk2.zip, WAS_V8.0_disk3.zip, WAS_V8.0_disk4.zip	Comma separated list of file names of the compressed WebSphere software packages.
WebSphere Binary Files	/opt/IBM/was	Fully qualified path where the compressed software will be extracted on the target machine. This location cannot be the same as Install Manager Extract Location.
WebSphere Extract Location	/opt/IBM/ WebSphere/AppServer	Fully qualified path where WebSphere will be installed.

Parameters for Provision WebSphere and Deployment Manager

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

Input Parameters Defined in this Step: Gather Parameters for WebSphere and Deployment Manager

Parameter Name	Default Value	Required	Description
Admin Password	no default	optional	When Enable Security is set to true, this parameter must contain a string that does not begin with a dash (-) or contain a space ( ).
Admin User	no default	optional	When Enable Security is set to true, this parameter must contain a string that does not begin with a dash(-), a period(.), or a space( ). It cannot contain any of the following characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }.
Call Wrapper	see description	required	Command that will execute this step (or subsequent steps) as a specific user. Defaults are: UNIX targets: `/opt/hp/dma/client/jython.sh` running as root Windows targets: `jython` running as Administrator
Cell Name	no default	optional	Unique cell name that does not contain any of the following special characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }. If you plan to federate into an existing cell later, make sure that this name is not the same as the existing cell name.
Enable Security	no default	optional	Enables administrative security. Must be set to either true or false. If Enable Security is true, the Admin User and Admin Password parameters must have values.
Host Name	Server.name	required	Hostname or IP address of the target machine.
Install Manager Binary Download Location	`/opt/IBM /iim`	required	Fully qualified path to where the compressed Install Manager software package will be downloaded on the target machine. For example: `/opt/IBM/iim`
Install Manager Binary Files	no default	required	Name of the compressed Install Manager software package.
Install Manager Extract Location	no default	required	Fully qualified path where the compressed software will be extracted on the target machine. This location cannot be the same as WebSphere Extract Location.

Input Parameters Defined in this Step: Gather Parameters for WebSphere and Deployment Manager, continued

Parameter Name	Default Value	Required	Description
Install Manager Install Location	no default	required	Fully qualified path where Install Manager will be installed. For example: `/opt/IBM/InstallManager`
License Acceptance	false	required	Acknowledges that the end user agrees to the IBM International Program License Agreement. This is set to false by default and must be set to true in order for the installation to continue.
Node Name	no default	required	Unique node name that cannot contain any of the following special characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }. If you plan to federate into an existing cell later, make sure that the name is unique within that cell.
Profile Name	no default	required	A unique profile name. It cannot begin with a period (.) and cannot contain any of the following special characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }.
Web Service Password	no default	required	Password for the discovery web service API.
Web Service User	no default	required	User capable of modifying the managed environment through the discovery web service API.
WebSphere Binary Download Location	`/opt/IBM/WAS`	required	Fully qualified path to the compressed WebSphere software package on the target machine.
WebSphere Binary Files	no default	required	Comma separated list of file names of the compressed WebSphere software packages.
WebSphere Extract Location	no default	required	Fully qualified path where the compressed software will be extracted on the target machine. This location cannot be the same as Install Manager Extract Location.
WebSphere Install Location	no default	required	Fully qualified path where WebSphere will be installed.
Windows Administrator Password	no default	required	The Windows Administrator password. Required for Windows.
Windows Administrator User	no default	required	This is the Windows Administrator user. Required for Windows.

Additional Input Parameters Defined in this Step: Gather Advanced Parameters for WebSphere and Deployment Manager

Parameter Name	Default Value	Required	Description
Cleanup on Failure	True	optional	Indicates whether to remove downloaded and extracted files and to clean up the installation directory in the event of workflow failure. Valid values are True and False. The default is True, which will clean up on failure.
Cleanup on Success	True	optional	Indicates whether to remove downloaded and extracted files and to clean up the installation directory in the event of workflow success. Valid values are True and False. The default is True, which will clean up on success.
Default Ports	false	optional	Provides the option to assign default ports to a profile. Valid values are true or false. If true, the WebSphere Application Server default ports will be used, and the Ports File and Starting Port parameters should not have values. If false, the workflow will increment the default port until it finds a free port. The default value is false.
Keystore Password	no default	optional	Sets the password for all keystore files created during profile creation. This includes keystore files for both the default personal certificate and the root signing certificate.
Omit Action	no default	optional	Enables you to prevent certain optional features from being installed. Valid values are deployAdminConsole or defaultAppDeployAndConfig. You may only specify one of these options.
Personal CertDN	no default	optional	Distinguished name of the personal certificate. For example: CN=dmalab-example.com,OU=WAS7LabCell, OU=WAS7LabDmgrManager,O=IBM,C=US The DN string cannot contain spaces. If you do not specify the DN, the WebSphere Application Server installer will create one.
Personal CertValidity Period	1	optional	Amount of time in years that the personal certificate is valid. Default is one year.
Ports File	no default	optional	Fully qualified path to a file that defines port settings for the new profile. This file must contain key=value pairs that specify a service name and a port number (for example: WC_adminhost=9060). This option should be used with the Validate Ports option.
Profile Response File	no default	optional	Fully qualified path where the response file that this workflow creates will be located. This file will then be used to drive the installation.
Response File	no default	optional	Fully qualified path where the response file that this workflow creates will be located. This file will then be used to drive the installation and profile creation.

Additional Input Parameters Defined in this Step: Gather Advanced Parameters for WebSphere and Deployment Manager, continued

Parameter Name	Default Value	Required	Description
Signing CertDN	no default	optional	Distinguished name of the signing certificate. For example: CN=dmalab-example.com, OU=Root Certificate, OU=WAS7TestLabCell, OU=WAS7LabNode1, O=IBM, C=US The DN string cannot contain spaces. If you do not specify the DN, the WebSphere Application Server installer will create one.
Signing CertValidity Period	15	optional	Amount of time in years that the root certificate is valid. Default is 15 years.
Starting Port	no default	optional	Starting port number that the profile will use to generate and assign port values. Port values are assigned sequentially from the Starting Port. Do not specify this parameter if you specify Default Ports or Ports File.
Validate Ports	no default	optional	Indicates that the ports should be validated to ensure that they are not already in use. Valid values are true or false. You should use this option if you specify a Ports File.

Provision WebSphere and Stand-Alone

Use this workflow to install the WebSphere 8.0 or 8.5.x Base core binaries and, optionally, create a stand-alone profile.

A stand-alone application server works independently—it is not part of a cell and does not interact with a deployment manager. The stand-alone profile is not suitable for distributed application server environments.

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

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

Note: The documentation for this workflow contains steps that are referred to by their base names. The names in the HPE DMA user interface may have a version appended, for example, v2.

Prerequisites for this Workflow

Be sure that the following prerequisites are satisfied before you run the Provision WebSphere and Stand-Alone

workflow:

1. This workflow requires unchallenged `sudo` access to a user (typically root) who can access all required files and directories.
2. Per the IBM WebSphere 8 documentation, the following system libraries are required before provisioning IBM WebSphere Application Server Network Deployment version 8.0 or 8.5.x on 64-bit and 32-bit Red Hat Linux targets:

Platform	Required Library
64-bit Red Hat Enterprise Linux version 5	compat-libstdc++-33-3.2.3-61 compat-db-4.2.52-5.1 gtk2-2.10.4-29.el5 gtk2-engines-2.8.0-3.el5 ksh-20080202-14 libXp-1.0.0-8 libXmu-1.0.2-5 libXtst-1.0.1-3.1 pam-0.99.6.2-3.26.el5 elfutils-0.125-3.el5 elfutils-libs-0.125-3.el5 libXft-2.1.10-1.1 libstdc++-4.1.2-48 If the target server supports both 32-bit and 64-bit applications then both the 32-bit and 64-bit versions of the following libraries are required: compat-libstdc++-33-3.2.3-61 compat-db-4.2.52-5.1 gtk2-2.18.9-4 gtk2-engines-2.18.4-5 libstdc++-4.1.2-48 libXft-2.1.10-1.1 libXp-1.0.0-8 libXmu-1.0.2-5 libXtst-1.0.1-3.1 pam-0.99.6.2-3.26.el5

Platform	Required Library
64-bit Red Hat Enterprise Linux version 6	compat-libstdc++-33-3.2.3-69 compat-db-4.6.21-15 ksh-20100621-2 gtk2-2.18.9-4 gtk2-engines-2.18.4-5 libXp-1.0.0-15.1 libXmu-1.0.5-1 libXtst-1.0.99.2-3 pam-1.1.1-4 elfutils-0.148-1 elfutils-libs-0.148-1 libXft-2.1.13-4.1 libstdc++-4.4.4-13 If the target server supports both 32-bit and 64-bit applications then both the 32-bit and 64-bit versions of the following libraries are required: compat-libstdc++-33-3.2.3-69 compat-db-4.6.21-15 libstdc++-4.4.4-13 libXp-1.0.0-15.1 libXmu-1.0.5-1 libXtst-1.0.99.2-3 pam-1.1.1-4 libXft-2.1.13-4.1 gtk2-2.18.9-4 gtk2-engines-2.18.4-5

Make sure that these libraries exist on each target server before running this workflow. If newer versions of these libraries are available, you can install the newer versions.

3. This workflow will install WebSphere Application Server as root because of the following IBM documented limitations:
   - Creation of a Linux service for WebSphere Application Server
   - Native registration with the operating system
   - Port conflicts that may occur with other installations of WebSphere Application Server that are not registered with the operating system

If there is a need to run as a non-root user after installation, you can run a recursive `chown` under the installation root and set owner permissions accordingly.

For more information about prerequisites for WebSphere 8, refer to the WebSphere 8 Product Documentation.

How this Workflow Works

This topic contains the following information about the "Provision WebSphere and Stand-Alone" workflow:

Overview

This workflow does the following three things in the order shown:

1. Installs the IBM Install Manager
2. Installs IBM WebSphere Application Server Network Deployment version 8.0 or 8.5.x
3. Creates a stand-alone profile

The workflow checks to see if the WebSphere 8.0 or 8.5.x binary archive files exist on the target machine. If they do not, the files are downloaded from the software repository.

See the following topics for detailed information:

Validation Checks Performed

Steps in this Workflow

Process Flow

Note: This workflow has been updated to account for the significant changes in the way that WebSphere 8 are installed.

Validation Checks Performed

Most of the validation centers on special characters and spaces in the parameters. There are also validation checks that happen at the operating system level, including file system space checks and RPM checks (on Red Hat Linux platforms only).

The workflow first performs the following parameter checks:

1. Required parameters have values specified.
2. WebSphere specific names do not contain the following characters: / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }
3. Parameters do not contain illegal characters for the parameter type.
4. Flag parameters are set to true or false.
5. Integer parameters are set to appropriate integer values.
6. Mutually dependent parameters are specified appropriately as a set.
7. Parameters are set to one of the values if the parameter has a list of valid values.
8. License Acceptance is true (for workflows that input the License Acceptance parameter).
9. All specified file names are legal file names.
10. All specified locations are legal path names. If they do not exist they will be created.

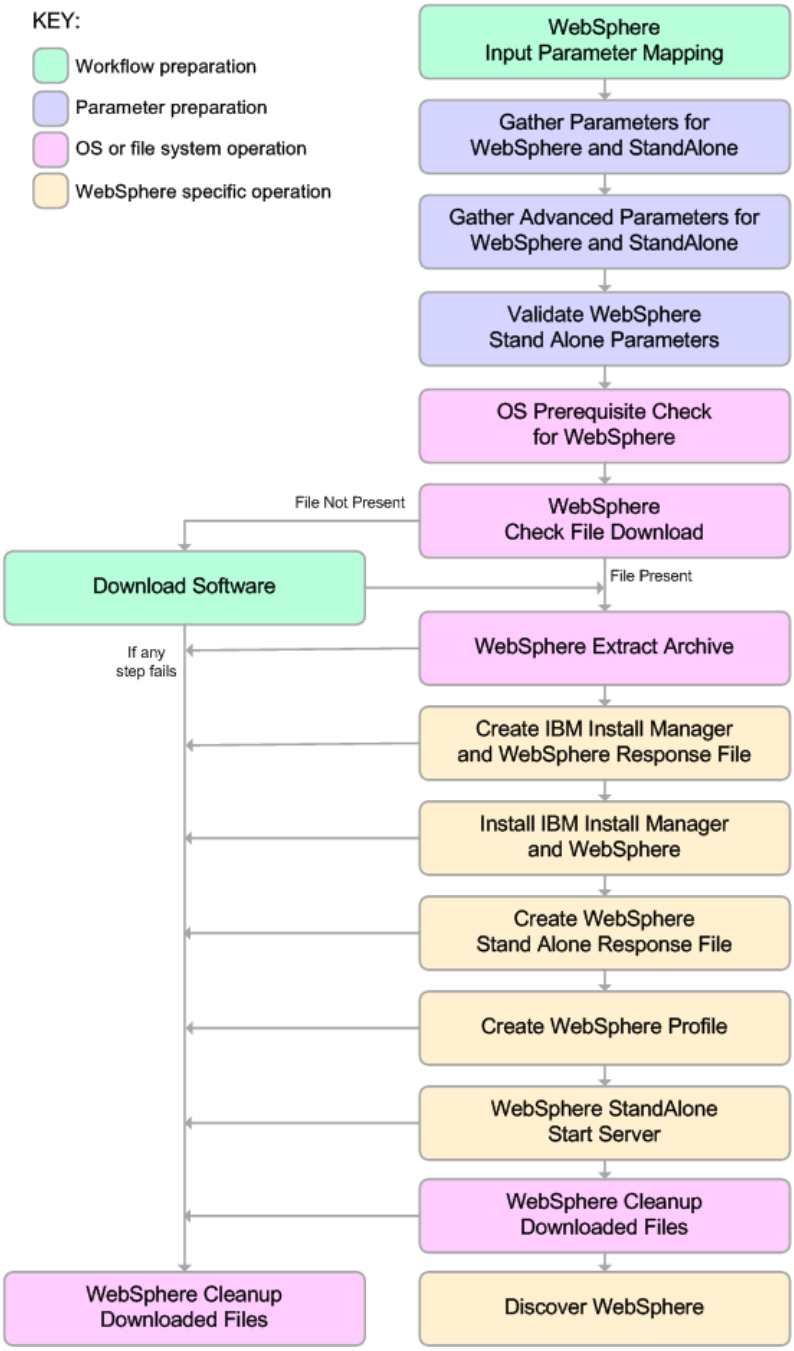
Note: For more information about valid parameter values, see "Parameters for Provision WebSphere and Stand-Alone".

The workflow then performs the following operating system checks on the target machine:

1. All required libraries are present (see "Prerequisites for this Workflow" on page 59).
2. Sufficient disk space is available to install WebSphere 8.0 or 8.5.x.
3. Sufficient disk space is available to extract the binary files from the compressed archive.

Steps Executed

The WebSphere 8.0 or 8.5.x workflow includes the following steps. Each step must complete successfully before the next step can start. If a step fails, the workflow reports a failure, and all subsequent steps are skipped.



Process Flow

This workflow performs the following tasks:

1. Creates the call wrapper and determines the target server platform type.
2. Gathers and validates the parameters needed to install WebSphere 8.0 or 8.5.x and create a stand-alone profile (see "Validation Checks Performed " on page 63).
3. Checks the following:
   a. Documented library requirements for WebSphere 8 (see the "Prerequisites for this Workflow" on page 59).
   b. File system space requirements where WebSphere 8.0 or 8.5.x will be installed.
   c. Temporary space requirements where the compressed software will be extracted before it is installed.
4. Determines whether the WebSphere 8.0 or 8.5.x binary archive is present on the target machine. If the archive is not present, the workflow downloads it from the software repository.
5. Extracts the WebSphere 8.0 or 8.5.x binary archive to the specified directory.
6. Creates a response file for the purpose of installing a new instance of WebSphere 8.0 or 8.5.x.
7. Installs the IBM Installation Manager and a new WebSphere 8.0 or 8.5.x instance on the target server.
8. Creates a new response file for the purpose of creating a stand-alone profile on top of the WebSphere 8.0 or 8.5.x installation.
9. Creates a stand-alone profile on top of the WebSphere 8.0 or 8.5.x installation.
10. Starts the new stand-alone WebSphere 8.0 or 8.5.x application server.
11. Cleans up any files that were downloaded—for either workflow success or failure.

    Note: The parameters Cleanup on Success and Cleanup on Failure are defaulted to True. If they are set to False, the downloaded files are not cleaned up.

12. Discovers any WebSphere 8.0 or 8.5.x cells, clusters, and managed servers associated with the Profile Root that you specify. If these items are found, they are added to the HPE DMA environment.

How to Run this Workflow

The following instructions show you how to customize and run the "Provision WebSphere and Stand-Alone" workflow in your environment.

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

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

To customize and run the Provision WebSphere and Stand-Alone workflow:

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

   Parameters Defined in this Step: Gather Parameters for WebSphere and StandAlone

Parameter Name	Default Value	Required	Description
Admin Password	no default	optional	When Enable Security is set to true, this parameter must contain a string that does not begin with a dash(-) or contain a space( ).
Admin User	no default	optional	When Enable Security is set to true, this parameter must contain a string that does not begin with a dash(-), a period(.), or a space( ). It cannot contain any of the following characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }.
Cell Name	no default	required	Unique cell name that does not contain any of the following special characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }. If you plan to federate into an existing cell later, make sure that this name is not the same as the existing cell name.
Enable Security	no default	required	Enables administrative security. Must be set to either true or false. If Enable Security is true, the Admin User and Admin Password parameters must have values.
Install Manager Binary Download Location	`/opt/IBM/iim`	required	Fully qualified path to where the compressed Install Manager software package will be downloaded on the target machine. For example: `/opt/IBM/iim`
Install Manager Binary Files	no default	required	Name of the compressed Install Manager software package.

Parameters Defined in this Step: Gather Parameters for WebSphere and StandAlone, continued

Parameter Name	Default Value	Required	Description
Install Manager Extract Location	no default	required	Fully qualified path where the compressed software will be extracted on the target machine. This location cannot be the same as Install Manager Install Location.
Install Manager Install Location	no default	required	Fully qualified path where Install Manager will be installed. For example: `/opt/IBM/InstallManager`
License Acceptance	false	required	Acknowledges that the end user agrees to the IBM International Program License Agreement. This is set to false by default and must be set to true in order for the installation to continue.
Node Name	no default	required	Unique node name that cannot contain any of the following special characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }. If you plan to federate into an existing cell later, make sure that the name is unique within that cell.
Profile Name	no default	required	A unique profile name. It cannot begin with a period (.) and cannot contain any of the following special characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }.
Server Name	no default	required	Name of the application server that will be created under the profile.
Web Service Password	no default	required	Password for the discovery web service API.
Web Service User	no default	required	User capable of modifying the managed environment through the discovery web service API.
WebSphere Binary Download Location	`/opt/IBM/WAS`	required	Fully qualified path to the compressed WebSphere software package on the target machine.
WebSphere Binary Files	no default	required	Comma separated list of file names of the compressed WebSphere software packages.
WebSphere Extract Location	no default	required	Fully qualified path where the compressed software will be extracted on the target machine. This location cannot be the same as Install Manager Extract Location.
WebSphere Install Location	no default	required	Fully qualified path where WebSphere will be installed.

Parameters Defined in this Step: Gather Parameters for WebSphere and StandAlone, continued

Parameter Name	Default Value	Required	Description
Windows Administrator Password	no default	required	The Windows Administrator password. Required for Windows.
Windows Administrator User	no default	required	This is the Windows Administrator user. Required for Windows.

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

See "Parameters for Provision WebSphere and Stand-Alone" for detailed descriptions of all input parameters for this workflow, including default values.

Tip: To avoid having to re-enter passwords whenever they change, you can create a policy to provide them to the workflow.

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

To verify the results:

Be sure to also perform the following steps:

1. After the workflow has completed, run the following command to check the version of WebSphere Application Server that was installed:

   WAS_ROOT/bin/versionInfo.sh

   Here, *WAS_ROOT* is the directory where WebSphere 8.0 or 8.5.x is installed. This is the path that you specified in the WebSphere Install Location parameter.
2. Validate that the profile has been created and is running by doing the following:
   a. View the *WAS_ROOT*/profiles/*PROFILE_NAME*/logs/AboutThisProfile.txt file. This file is created after the creation of the profile and contains specific information about the profile.

      Here, *PROFILE_NAME* is the name of the profile that you just created. This is the name that you specified in the Profile Name parameter.
   b. Change to the *WAS_ROOT*/profiles/*PROFILE_NAME*/logs/*CELL_NAME* directory, and tail the SystemOut.log file. Look for the following line:

      Server *CELL_NAME* open for e-business

      Here, *CELL_NAME* is the name of the WebSphere 8.0 or 8.5.x cell to which this profile pertains. This is the name that you specified in the Cell Name parameter.

Sample Scenario

This topic shows you typical parameter values used for the "Provision WebSphere and Stand-Alone" workflow.

Tip: To avoid having to re-enter passwords whenever they change, you can create a policy to provide them to the workflow.

New Install with Stand-Alone Profile – Parameter Value Examples

Parameter Name	Example Value	Description
Admin Password	wasPassWord	When Enable Security is set to true, this parameter must contain a string that does not begin with a dash(-) or contain a space( ).
Admin User	wasadmin	When Enable Security is set to true, this parameter must contain a string that does not begin with a dash(-), a period(.), or a space( ). It cannot contain any of the following characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }.
Cell Name	DevCell	Unique cell name that does not contain any of the following special characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }. If you plan to federate into an existing cell later, make sure that this name is not the same as the existing cell name.
Enable Security	true	Enables administrative security. Must be set to either true or false. If Enable Security is true, the Admin User and Admin Password parameters must have values.
Install Manager Binary Download Location	/opt/IBM/iim	Fully qualified path to where the compressed Install Manager software package will be downloaded on the target machine. For example: `/opt/IBM/iim`
Install Manager Binary Files	IBM_Install_Manager_Linux.zip	Name of the compressed Install Manager software package.
Install Manager Extract Location	/opt/IBM/iim	Fully qualified path where the compressed software will be extracted on the target machine. This location cannot be the same as WebSphere Extract Location.
Install Manager Install Location	/opt/IBM/installManager	Fully qualified path where Install Manager will be installed. For example: `/opt/IBM/InstallManager`
License Acceptance	true	Acknowledges that the end user agrees to the IBM International Program License Agreement. This is set to false by default and must be set to true in order for the installation to continue.

New Install with Stand-Alone Profile – Parameter Value Examples, continued

Parameter Name	Example Value	Description
Node Name	DevNode	Unique node name that cannot contain any of the following special characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }. If you plan to federate into an existing cell later, make sure that the name is unique within that cell.
Profile Name	standAlone	A unique profile name. It cannot begin with a period (.) and cannot contain any of the following special characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }.
Server Name	Server1	Name of the application server that will be created under the profile.
Web Service Password	myWebSvcPwd	Password for the discovery web service API.
Web Service User	JohnDoe	User capable of modifying the managed environment through the discovery web service API.
WebSphere Binary Download Location	/opt/IBM/was	Fully qualified path to the compressed WebSphere software package on the target machine.
WebSphere Binary Files	WAS_V8.0_disk1.zip, WAS_V8.0_disk2.zip	Comma separated list of file names of the compressed WebSphere software packages.
WebSphere Extract Location	/opt/IBM/was	Fully qualified path where the compressed software will be extracted on the target machine. This location cannot be the same as Install Manager Extract Location.
WebSphere Install Location	/opt/IBM/ WebSphere/AppServer	Fully qualified path where WebSphere will be installed.

Parameters for Provision WebSphere and Stand-Alone

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

Input Parameters Defined in this Step: Gather Parameters for WebSphere and StandAlone

Parameter Name	Default Value	Required	Description
Admin Password	no default	optional	When Enable Security is set to true, this parameter must contain a string that does not begin with a dash(-) or contain a space( ).
Admin User	no default	optional	When Enable Security is set to true, this parameter must contain a string that does not begin with a dash(-), a period(.), or a space( ). It cannot contain any of the following characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }.
Call Wrapper	see description	required	Command that will execute this step (or subsequent steps) as a specific user. Defaults are: UNIX targets: `/opt/hp/dma/client/jython.sh` running as root Windows targets: `jython` running as Administrator
Cell Name	no default	required	Unique cell name that does not contain any of the following special characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }. If you plan to federate into an existing cell later, make sure that this name is not the same as the existing cell name.
Enable Security	no default	required	Enables administrative security. Must be set to either true or false. If Enable Security is true, the Admin User and Admin Password parameters must have values.
Host Name	Server.name	required	Hostname or IP address of the target machine.
Install Manager Binary Download Location	`/opt/IBM /iim`	required	Fully qualified path to where the compressed Install Manager software package will be downloaded on the target machine. For example: `/opt/IBM/iim`
Install Manager Binary Files	no default	required	Name of the compressed Install Manager software package.
Install Manager Extract Location	no default	required	Fully qualified path where the compressed software will be extracted on the target machine. This location cannot be the same as WebSphere Extract Location.
Install	no default	required	Fully qualified path where Install Manager will be installed. For

Input Parameters Defined in this Step: Gather Parameters for WebSphere and StandAlone, continued

Parameter Name	Default Value	Required	Description
Manager Install Location			example: `/opt/IBM/InstallManager`
License Acceptance	false	required	Acknowledges that the end user agrees to the IBM International Program License Agreement. This is set to false by default and must be set to true in order for the installation to continue.
Node Name	no default	required	Unique node name that cannot contain any of the following special characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }. If you plan to federate into an existing cell later, make sure that the name is unique within that cell.
Profile Name	no default	required	A unique profile name. It cannot begin with a period (.) and cannot contain any of the following special characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }.
Server Name	no default	required	Name of the application server that will be created under the profile.
Web Service Password	no default	required	Password for the discovery web service API.
Web Service User	no default	required	User capable of modifying the managed environment through the discovery web service API.
WebSphere Binary Download Location	`/opt/IBM/WAS`	required	Fully qualified path to the compressed WebSphere software package on the target machine.
WebSphere Binary Files	no default	required	Comma separated list of file names of the compressed WebSphere software packages.
WebSphere Extract Location	no default	required	Fully qualified path where the compressed software will be extracted on the target machine. This location cannot be the same as Install Manager Extract Location.
WebSphere Install Location	no default	required	Fully qualified path where WebSphere will be installed.
Windows Administrator Password	no default	required	The Windows Administrator password. Required for Windows.
Windows Administrator User	no default	required	This is the Windows Administrator user. Required for Windows.

Additional Input Parameters Defined in this Step: Gather Advanced Parameters for WebSphere and StandAlone

Parameter Name	Default Value	Required	Description
Cleanup on Failure	True	optional	Indicates whether to remove downloaded and extracted files and to clean up the installation directory in the event of workflow failure. Valid values are True and False. The default is True, which will clean up on failure.
Cleanup on Success	True	optional	Indicates whether to remove downloaded and extracted files and to clean up the installation directory in the event of workflow success. Valid values are True and False. The default is True, which will clean up on success.
Default Ports	false	optional	Provides the option to assign default ports to a profile. Valid values are true or false. If true, the WebSphere Application Server default ports will be used, and the Ports File and Starting Port parameters should not have values. If false, the workflow will increment the default port until it finds a free port. The default value is false.
Developer Server	no default	optional	Use this parameter for development environments only to help with start up time. Valid value is true. Do not use in production environments.
Keystore Password	no default	optional	Sets the password for all keystore files created during profile creation. This includes keystore files for both the default personal certificate and the root signing certificate.
Omit Action	no default	optional	Enables you to prevent certain optional features from being installed. Valid values are deployAdminConsole or defaultAppDeployAndConfig. You may only specify one of these options.
Personal CertDN	no default	optional	Distinguished name of the personal certificate. For example: CN=dmalab-example.com,OU=WAS7LabCell, OU=WAS7LabDmgrManager,O=IBM,C=US The DN string cannot contain spaces. If you do not specify the DN, the WebSphere Application Server installer will create one.
Personal CertValidity Period	1	optional	Amount of time in years that the personal certificate is valid. Default is one year.
Ports File	no default	optional	Fully qualified path to a file that defines port settings for the new profile. This file must contain key=value pairs that specify a service name and a port number (for example: WC_adminhost=9060). This option should be used with the Validate Ports option.
Profile Response File	no default	optional	Fully qualified path where the response file that this workflow creates will be located. This file will then be used to drive the installation.

Additional Input Parameters Defined in this Step: Gather Advanced Parameters for WebSphere and StandAlone, continued

Parameter Name	Default Value	Required	Description
Response File	no default	optional	Fully qualified path where the response file that this workflow creates will be located. This file will then be used to drive the installation and profile creation.
Signing CertDN	no default	optional	Distinguished name of the signing certificate. For example: CN=dmalab-example.com, OU=Root Certificate, OU=WAS7TestLabCell, OU=WAS7LabNode1, O=IBM, C=US The DN string cannot contain spaces. If you do not specify the DN, the WebSphere Application Server installer will create one.
Signing CertValidity Period	15	optional	Amount of time in years that the root certificate is valid. Default is 15 years.
Starting Port	no default	optional	Starting port number that the profile will use to generate and assign port values. Port values are assigned sequentially from the Starting Port. Do not specify this parameter if you specify Default Ports or Ports File.
Validate Ports	no default	optional	Indicates that the ports should be validated to ensure that they are not already in use. Valid values are true or false. You should use this option if you specify a Ports File.

Provision WebSphere Stand-Alone Profile From Existing Install

Use this workflow to create a stand-alone profile on an existing WebSphere 8.0 or 8.5.x installation.

A stand-alone application server works independently—it is not part of a cell and does not interact with a deployment manager. The stand-alone profile is not suitable for distributed application server environments.

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

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

Prerequisites for this Workflow

Be sure that the following prerequisites are satisfied before you run the Provision WebSphere Stand-Alone Profile From Existing Install

workflow:

1. This workflow requires unchallenged `sudo` access to a user (typically root) who can access all required files and directories.
2. Per the IBM WebSphere 8 documentation, the following system libraries are required before provisioning IBM WebSphere Application Server Network Deployment version 8.0 or 8.5.x on 64-bit and 32-bit Red Hat Linux targets:

Platform	Required Library
64-bit Red Hat Enterprise Linux version 5	compat-libstdc++-33-3.2.3-61 compat-db-4.2.52-5.1 gtk2-2.10.4-29.el5 gtk2-engines-2.8.0-3.el5 ksh-20080202-14 libXp-1.0.0-8 libXmu-1.0.2-5 libXtst-1.0.1-3.1 pam-0.99.6.2-3.26.el5 elfutils-0.125-3.el5 elfutils-libs-0.125-3.el5 libXft-2.1.10-1.1 libstdc++-4.1.2-48 If the target server supports both 32-bit and 64-

Platform	Required Library
	bit applications then both the 32-bit and 64-bit versions of the following libraries are required: compat-libstdc++-33-3.2.3-61 compat-db-4.2.52-5.1 gtk2-2.18.9-4 gtk2-engines-2.18.4-5 libstdc++-4.1.2-48 libXft-2.1.10-1.1 libXp-1.0.0-8 libXmu-1.0.2-5 libXtst-1.0.1-3.1 pam-0.99.6.2-3.26.el5
64-bit Red Hat Enterprise Linux version 6	compat-libstdc++-33-3.2.3-69 compat-db-4.6.21-15 ksh-20100621-2 gtk2-2.18.9-4 gtk2-engines-2.18.4-5 libXp-1.0.0-15.1

Platform	Required Library
	libXmu-1.0.5-1 libXtst-1.0.99.2-3 pam-1.1.1-4 elfutils-0.148-1 elfutils-libs-0.148-1 libXft-2.1.13-4.1 libstdc++-4.4.4-13 If the target server supports both 32-bit and 64-bit applications then both the 32-bit and 64-bit versions of the following libraries are required: compat-libstdc++-33-3.2.3-69 compat-db-4.6.21-15 libstdc++-4.4.4-13 libXp-1.0.0-15.1 libXmu-1.0.5-1

Platform	Required Library
	libXtst-1.0.99.2-3 pam-1.1.1-4 libXft-2.1.13-4.1 gtk2-2.18.9-4 gtk2-engines-2.18.4-5

Make sure that these libraries exist on each target server before running this workflow. If newer versions of these libraries are available, you can install the newer versions.

3. This workflow will install WebSphere Application Server as root because of the following IBM documented limitations:
   - Creation of a Linux service for WebSphere Application Server
   - Native registration with the operating system
   - Port conflicts that may occur with other installations of WebSphere Application Server that are not registered with the operating system

   If there is a need to run as a non-root user after installation, you can run a recursive `chown` under the installation root and set owner permissions accordingly.

For more information about prerequisites for WebSphere 8, refer to the WebSphere 8 Product Documentation.

How this Workflow Works

This topic contains the following information about the "Provision WebSphere Stand-Alone Profile From Existing Install" workflow:

Overview

This workflow creates a stand-alone profile on an existing WebSphere 8.0 or 8.5.x installation.

See the following topics for detailed information:

Validation Checks Performed

Steps in this Workflow

Process Flow

Validation Checks Performed

Most of the validation centers on special characters and spaces in the parameters. There are also validation checks that happen at the operating system level, including file system space checks and RPM checks (on Red Hat Linux platforms only).

The workflow first performs the following parameter checks:

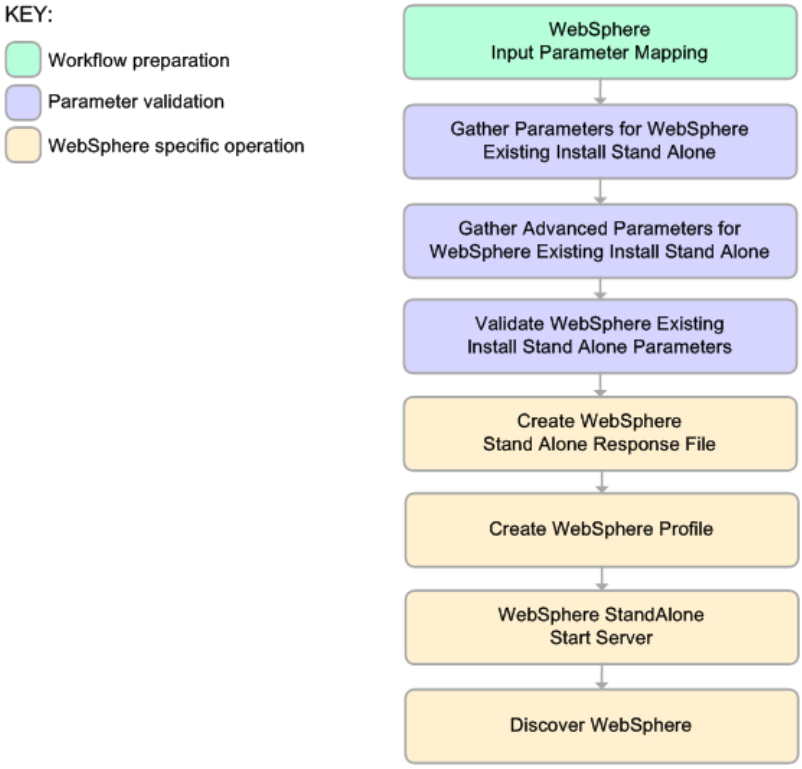
1. Required parameters have values specified.
2. WebSphere specific names do not contain the following characters: / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }
3. Parameters do not contain illegal characters for the parameter type.
4. Flag parameters are set to true or false.
5. Integer parameters are set to appropriate integer values.
6. Mutually dependent parameters are specified appropriately as a set.
7. Parameters are set to one of the values if the parameter has a list of valid values.
8. License Acceptance is true (for workflows that input the License Acceptance parameter).
9. All specified file names are legal file names.
10. All specified locations are legal path names. If they do not exist they will be created.

Note: For more information about valid parameter values, see "Parameters for Provision WebSphere Stand-Alone Profile from Existing Install".

The workflow then checks to make sure that all required libraries are present on the target machine (see "Prerequisites for this Workflow").

Steps Executed

The Provision WebSphere Stand-Alone Profile From Existing Install workflow includes the following steps. Each step must complete successfully before the next step can start. If a step fails, the workflow reports a failure, and all subsequent steps are skipped.



Process Flow

This workflow performs the following tasks:

1. Creates the call wrapper and determines the target server platform type.
2. Gathers and validates the parameters needed to create a stand-alone profile (see "Validation Checks Performed " on the previous page).
3. Creates a new response file for the purpose of creating a stand-alone profile on top of the existing WebSphere 8.0 or 8.5.x installation.
4. Creates a stand-alone profile on top of the WebSphere 8.0 or 8.5.x installation.
5. Starts the stand-alone application server.
6. Discovers any WebSphere 8.0 or 8.5.x cells, clusters, and managed servers associated with the Profile Root that you specify. If these items are found, they are added to the HPE DMA environment.

How to Run this Workflow

The following instructions show you how to customize and run the "Provision WebSphere Stand-Alone Profile From Existing Install" workflow in your environment.

The workflow provides default values for some parameters. These default values are usually sufficient for a "typical" installation. You can override the defaults by specifying parameter values in the deployment. You can also expose additional parameters in the workflow, if necessary, to accomplish more advanced scenarios. Any parameters not explicitly specified in the deployment will have the default values listed in "Parameters for Provision WebSphere Stand-Alone Profile from Existing Install".

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

To customize and run the Provision WebSphere Stand-Alone Profile From Existing Install workflow:

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

   Parameters Defined in this Step: Gather Parameters for WebSphere Existing Install Stand Alone

Parameter Name	Default Value	Required	Description
Admin Password	no default	optional	When Enable Security is set to true, this parameter must contain a string that does not begin with a dash(-) or contain a space( ).
Admin User	no default	optional	When Enable Security is set to true, this parameter must contain a string that does not begin with a dash(-), a period(.), or a space( ). It cannot contain any of the following characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }.
Cell Name	no default	required	Unique cell name that does not contain any of the following special characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }. If you plan to federate into an existing cell later, make sure that this name is not the same as the existing cell name.
Enable Security	no default	required	Enables administrative security. Must be set to either true or false. If Enable Security is true, the Admin User and Admin Password parameters must have values.
Node Name	no default	required	Unique node name that cannot contain any of the following special characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }. If you plan to federate into an existing cell later, make sure that the name is unique within that cell.
Profile Name	no default	required	A unique profile name. It cannot begin with a period (.) and cannot contain any of the following special characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }.

Parameters Defined in this Step: Gather Parameters for WebSphere Existing Install Stand Alone, continued

Parameter Name	Default Value	Required	Description
Server Name	no default	required	Name of the application server that will be created under the profile.
Web Service Password	no default	required	Password for the discovery web service API.
Web Service User	no default	required	User capable of modifying the managed environment through the discovery web service API.
WebSphere Install Location	no default	required	Fully qualified path where WebSphere will be installed.
Windows Administrator Password	no default	required	The Windows Administrator password. Required for Windows.
Windows Administrator User	no default	required	This is the Windows Administrator user. Required for Windows.

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

See "Parameters for Provision WebSphere Stand-Alone Profile from Existing Install" for detailed descriptions of all input parameters for this workflow, including default values.

Tip: To avoid having to re-enter passwords whenever they change, you can create a policy to provide them to the workflow.

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

To verify the results:

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

Be sure to also perform the following steps:

1. After the workflow has completed, run the following command to check the version of WebSphere Application Server that was installed:

   WAS_ROOT/bin/versionInfo.sh

   Here, *WAS_ROOT* is the directory where WebSphere 8.0 or 8.5.x is installed. This is the path that you specified in the WebSphere Install Location parameter.
2. Validate that the profile has been created and is running by doing the following:
   a. View the *WAS_ROOT*/profiles/*PROFILE_NAME*/logs/AboutThisProfile.txt file. This file is created after the creation of the profile and contains specific information about the profile.

      Here, *PROFILE_NAME* is the name of the profile that you just created. This is the name that you specified in the Profile Name parameter.

   b. Change to the *WAS_ROOT*/profiles/*PROFILE_NAME*/logs/*CELL_NAME* directory, and tail the SystemOut.log file. Look for the following line:

      Server *CELL_NAME* open for e-business

      Here, *CELL_NAME* is the name of the WebSphere 8.0 or 8.5.x cell to which this profile pertains. This is the name that you specified in the Cell Name parameter.

Sample Scenario

This topic shows you typical parameter values used for the "Provision WebSphere Stand-Alone Profile From Existing Install" workflow.

Tip: To avoid having to re-enter passwords whenever they change, you can create a policy to provide them to the workflow.

Stand-Alone Profile on Existing Install – Parameter Value Examples

Parameter Name	Example Value	Description
Admin Password	wasPassWord	When Enable Security is set to true, this parameter must contain a string that does not begin with a dash(-) or contain a space( ).
Admin User	wasadmin	When Enable Security is set to true, this parameter must contain a string that does not begin with a dash(-), a period(.), or a space( ). It cannot contain any of the following characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }.
Cell Name	DevStandAlone1Cell	Unique cell name that does not contain any of the following special characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }. If you plan to federate into an existing cell later, make sure that this name is not the same as the existing cell name.
Enable Security	true	Enables administrative security. Must be set to either true or false. If Enable Security is true, the Admin User and Admin Password parameters must have values.
Node Name	DevStandAlone1Node	Unique node name that cannot contain any of the following special characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }. If you plan to federate into an existing cell later, make sure that the name is unique within that cell.
Profile Name	StandAlone1	A unique profile name. It cannot begin with a period (.) and cannot contain any of the following special characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }.
Server Name	Server1	Name of the application server that will be created under the profile.
Web Service Password	myWebSvcPwd	Password for the discovery web service API.
Web Service User	JohnDoe	User capable of modifying the managed environment through the discovery web service API.

Stand-Alone Profile on Existing Install – Parameter Value Examples, continued

Parameter Name	Example Value	Description
WebSphere Install Location	/opt/IBM/ WebSphere/AppServer	Fully qualified path where WebSphere will be installed.

Parameters for Provision WebSphere Stand-Alone Profile from Existing Install

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

Input Parameters Defined in this Step: Gather Parameters for WebSphere Existing Install Stand Alone

Parameter Name	Default Value	Required	Description
Admin Password	no default	optional	When Enable Security is set to true, this parameter must contain a string that does not begin with a dash(-) or contain a space( ).
Admin User	no default	optional	When Enable Security is set to true, this parameter must contain a string that does not begin with a dash(-), a period(.), or a space( ). It cannot contain any of the following characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }.
Call Wrapper	see description	required	Command that will execute this step (or subsequent steps) as a specific user. Defaults are: UNIX targets: `/opt/hp/dma/client/jython.sh` running as root Windows targets: `jython` running as Administrator
Cell Name	no default	required	Unique cell name that does not contain any of the following special characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }. If you plan to federate into an existing cell later, make sure that this name is not the same as the existing cell name.
Enable Security	no default	required	Enables administrative security. Must be set to either true or false. If Enable Security is true, the Admin User and Admin Password parameters must have values.
Host Name	Server.name	required	Hostname or IP address of the target machine.
Node Name	no default	required	Unique node name that cannot contain any of the following special characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }. If you plan to federate into an existing cell later, make sure that the name is unique within that cell.
Profile Name	no default	required	A unique profile name. It cannot begin with a period (.) and cannot contain any of the following

Input Parameters Defined in this Step: Gather Parameters for WebSphere Existing Install Stand Alone, continued

Parameter Name	Default Value	Required	Description
			special characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }.
Server Name	no default	required	Name of the application server that will be created under the profile.
Web Service Password	no default	required	Password for the discovery web service API.
Web Service User	no default	required	User capable of modifying the managed environment through the discovery web service API.
WebSphere Install Location	no default	required	Fully qualified path where WebSphere will be installed.
Windows Administrator Password	no default	required	The Windows Administrator password. Required for Windows.
Windows Administrator User	no default	required	This is the Windows Administrator user. Required for Windows.

Additional Input Parameters Defined in this Step: Gather Advanced Parameters for WebSphere Existing Install Stand Alone

Parameter Name	Default Value	Required	Description
Default Ports	false	optional	Provides the option to assign default ports to a profile. Valid values are true or false. If true, the WebSphere Application Server default ports will be used, and the Ports File and Starting Port parameters should not have values. If false, the workflow will increment the default port until it finds a free port. The default value is false.
Developer Server	no default	optional	Use this parameter for development environments only to help with start up time. Valid value is true. Do not use in production environments.
Keystore Password	no default	optional	Sets the password for all keystore files created during profile creation. This includes keystore files for both the default personal certificate and the root signing certificate.
Omit Action	no default	optional	Enables you to prevent certain optional features from being installed. Valid values are deployAdminConsole or defaultAppDeployAndConfig. You may only specify one of these options.

Additional Input Parameters Defined in this Step: Gather Advanced Parameters for WebSphere Existing Install Stand Alone, continued

Parameter Name	Default Value	Required	Description
Personal CertDN	no default	optional	Distinguished name of the personal certificate. For example: CN=dmalab-example.com,OU=WAS7LabCell, OU=WAS7LabDmgrManager,O=IBM,C=US The DN string cannot contain spaces. If you do not specify the DN, the WebSphere Application Server installer will create one.
Personal CertValidity Period	1	optional	Amount of time in years that the personal certificate is valid. Default is one year.
Ports File	no default	optional	Fully qualified path to a file that defines port settings for the new profile. This file must contain key=value pairs that specify a service name and a port number (for example: WC_adminhost=9060). This option should be used with the Validate Ports option.
Profile Response File	no default	optional	Fully qualified path where the response file that this workflow creates will be located. This file will then be used to drive the installation.
Signing CertDN	no default	optional	Distinguished name of the signing certificate. For example: CN=dmalab-example.com, OU=Root Certificate, OU=WAS7TestLabCell, OU=WAS7LabNode1, O=IBM, C=US The DN string cannot contain spaces. If you do not specify the DN, the WebSphere Application Server installer will create one.
Signing CertValidity Period	15	optional	Amount of time in years that the root certificate is valid. Default is 15 years.
Starting Port	no default	optional	Starting port number that the profile will use to generate and assign port values. Port values are assigned sequentially from the Starting Port. Do not specify this parameter if you specify Default Ports or Ports File.
Validate Ports	no default	optional	Indicates that the ports should be validated to ensure that they are not already in use. Valid values are true or false. You should use this option if you specify a Ports File.

Provision IBM HTTP Server and Plug-in

Use this workflow to install IBM HTTP Server for WebSphere Application Server version 8.0 or 8.5.x and the plug-in on a target system and then to configure a Web server instance along with the plug-in on the same target system.

IBM HTTP Server version 8.0 or 8.5.x is a Web server that will serve both static and dynamic content. Usually you will front your WebSphere Application Server environment with an IBM HTTP Server.

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

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

Note: The documentation for this workflow contains steps that are referred to by their base names. The names in the HPE DMA user interface may have a version appended, for example, v2.

Prerequisites for this Workflow

Be sure that the following prerequisites are satisfied before you run the Provision IBM HTTP Server and Plug-in workflow:

1. This workflow requires unchallenged sudo access to a user (typically root) who can access all required files and directories.
2. Per the IBM WebSphere 8 documentation, the following system libraries are required before provisioning IBM WebSphere Application Server Network Deployment version 8.0 or 8.5.x on 64-bit and 32-bit Red Hat Linux targets:

Platform	Required Library
64-bit Red Hat Enterprise Linux version 5	compat-libstdc++-33-3.2.3-61 compat-db-4.2.52-5.1 gtk2-2.10.4-29.el5 gtk2-engines-2.8.0-3.el5 ksh-20080202-14 libXp-1.0.0-8 libXmu-1.0.2-5 libXtst-1.0.1-3.1 pam-0.99.6.2-3.26.el5 elfutils-0.125-3.el5 elfutils-libs-0.125-3.el5 libXft-2.1.10-1.1 libstdc++-4.1.2-48 If the target server supports both 32-bit and 64-bit applications then both the 32-bit and 64-bit versions of the following libraries are required: compat-libstdc++-33-3.2.3-61 compat-db-4.2.52-5.1 gtk2-2.18.9-4 gtk2-engines-2.18.4-5 libstdc++-4.1.2-48 libXft-2.1.10-1.1 libXp-1.0.0-8 libXmu-1.0.2-5 libXtst-1.0.1-3.1 pam-0.99.6.2-3.26.el5
64-bit Red Hat Enterprise Linux version 6	compat-libstdc++-33-3.2.3-69 compat-db-4.6.21-15 ksh-20100621-2 gtk2-2.18.9-4 gtk2-engines-2.18.4-5 libXp-1.0.0-15.1 libXmu-1.0.5-1

Platform	Required Library
	libXtst-1.0.99.2-3 pam-1.1.1-4 elfutils-0.148-1 elfutils-libs-0.148-1 libXft-2.1.13-4.1 libstdc++-4.4.4-13 If the target server supports both 32-bit and 64-bit applications then both the 32-bit and 64-bit versions of the following libraries are required: compat-libstdc++-33-3.2.3-69 compat-db-4.6.21-15 libstdc++-4.4.4-13 libXp-1.0.0-15.1 libXmu-1.0.5-1 libXtst-1.0.99.2-3 pam-1.1.1-4 libXft-2.1.13-4.1 gtk2-2.18.9-4 gtk2-engines-2.18.4-5

Make sure that these libraries exist on each target server before running this workflow. If newer versions of these libraries are available, you can install the newer versions.

For more information about prerequisites for WebSphere 8, refer to the WebSphere 8 Product Documentation.

How this Workflow Works

This topic contains the following information about the "Provision IBM HTTP Server and Plug-in" workflow:

Overview

This workflow does the following these things in the order shown:

1. Installs the IBM Install Manager
2. Installs IBM HTTP Server version 8.0 or 8.5.x and the plug-in
3. Configures a Web server instance
4. Creates a plug-in configuration for the Web server instance
5. Optionally, creates the HTTP admin instance
6. Optionally, runs all Web server instances and the HTTP admin instance as a non-root system account
7. Starts the Web server instance and, if configured, starts the HTTP admin instance
8. Discovers all IBM HTTP Server instances and populates HPE DMA with the relevant configuration information

The workflow checks to see if the IBM HTTP Server version 8.0 or 8.5.x binary archive files exist on the target machine. If they do not, the files are downloaded from the software repository.

See the following topics for detailed information:

Validation Checks Performed

Steps in this Workflow

Process Flow

Note: This workflow has been updated to account for the significant changes in the way that WebSphere 8 are installed.

Validation Checks Performed

Most of the validation centers on special characters and spaces in the parameters. There are also validation checks that happen at the operating system level, including file system space checks and RPM checks (on Red Hat Linux platforms only).

The workflow first performs the following parameter checks:

1. Required parameters have values specified.
2. WebSphere specific names do not contain the following characters: / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }
3. Parameters do not contain illegal characters for the parameter type.
4. Flag parameters are set to true or false.
5. Integer parameters are set to appropriate integer values.
6. Mutually dependent parameters are specified appropriately as a set.
7. Parameters are set to one of the values if the parameter has a list of valid values.
8. License Acceptance is true (for workflows that input the License Acceptance parameter).
9. All specified file names are legal file names.
10. All specified locations are legal path names. If they do not exist they will be created.

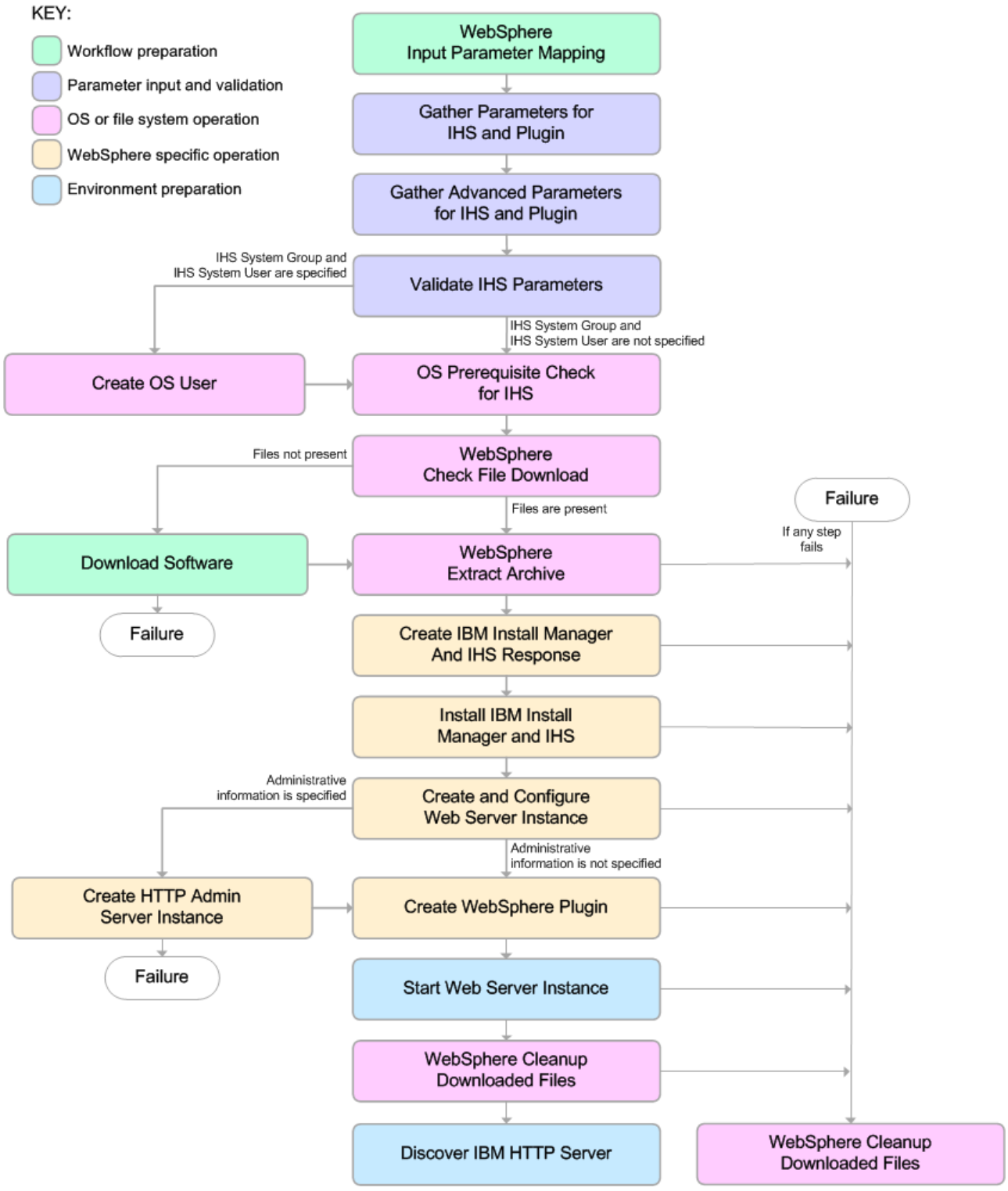
Note: For more information about valid parameter values, see "Parameters for Provision IBM HTTP Server and Plug-in".

The workflow then performs the following operating system checks on the target machine:

1. All required libraries are present (see "Prerequisites for this Workflow").
2. Sufficient disk space is available to install IBM HTTP Server for WebSphere Application Server version 8.0 or 8.5.x.
3. Sufficient disk space is available to extract the binary files from the compressed archive.

Steps Executed

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



Process Flow

This workflow performs the following tasks:

1. Creates the call wrapper to facilitate the execution of subsequent steps.
2. Gathers and validates the parameters needed to install IBM HTTP Server version 8.0 or 8.5.x and the plug-in (see "Validation Checks Performed " on page 95).
3. *Optional:* Creates the operating system user—if IHS System User and IHS System Group are specified.
4. Checks the following:
   a. Documented library requirements for IBM HTTP Server versions 8.0 and 8.5.x (see the "Prerequisites for this Workflow").
   b. File system space requirements where IBM HTTP Server version 8.0 or 8.5.x will be installed.
   c. Temporary space requirements where the compressed software will be extracted before it is installed.
5. Determines whether the IBM HTTP Server version 8.0 or 8.5.x binary archive and the Install Manager binary archive are present on the target machine. If the files are not present, the workflow downloads them from the software repository.
6. Extracts the IBM HTTP Server version 8.0 or 8.5.x and Install Manager binary archives to the specified directories.
7. Creates a response file for the purpose of installing the IBM Install Manager, a new IBM HTTP Server version 8.0 or 8.5.x instance, and the WebSphere plug-in.
8. Installs the IBM Installation Manager, a new IBM HTTP Server version 8.0 or 8.5.x instance, and the WebSphere plug-in on the target server.
9. Creates a new Web server instance under the installation root of IBM HTTP Server.
10. *Optional:* Creates the HTTP Admin Web server instance—if HTTP Admin User, HTTP Admin Password, and HTTP Admin Port are specified.
11. Creates the plug-in configuration files and plug-in log directory.
12. Starts the Web server instance.
13. Cleans up any files that were downloaded—for either workflow success or failure.

    Note: The parameters Cleanup on Success and Cleanup on Failure are defaulted to True. If they are set to False, the downloaded files are not cleaned up.

14. Discovers all IBM HTTP Server instances and populates HPE DMA with the relevant configuration information.

How to Run this Workflow

The following instructions show you how to customize and run the "Provision IBM HTTP Server and Plug-in" workflow in your environment.

The workflow provides default values for some parameters. These default values are usually sufficient for a "typical" installation. You can override the defaults by specifying parameter values in the deployment. You can also expose additional parameters in the workflow, if necessary, to accomplish more advanced scenarios. Any parameters not explicitly specified in the deployment will have the default values listed in "Parameters for Provision IBM HTTP Server and Plug-in".

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

To customize and run the Provision IBM HTTP Server and Plug-in workflow:

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

   Parameters Defined in this Step: Gather Parameters for IHS and Plugin

Parameter Name	Default Value	Required	Description
Http Port	80	required	The port on which the Web server will listen. Default is set to 80. If the Web server instance is run as non-root this value has to be greater than 1024.
IHS Binary Download Location	no default	required	Name of the compressed IHS software package.
IHS Binary Files	no default	required	Name of the compressed IHS software package.
IHS Extract Location	no default	required	Fully-qualified path where the compressed software will be extracted on the target machine. This cannot be the same as the Install Manager Extract Location.
IHS Install Location	no default	required	Fully-qualified path where IHS will be installed.
Install Manager Binary Download Location	no default	required	Fully-qualified path to the compressed Install Manager software package on the target machine.
Install Manager Binary Files	no default	required	Name of the compressed Install Manager software package.
Install Manager Extract	no default	required	Fully-qualified path where the compressed software will be extracted on the target machine. This location cannot be the

Parameters Defined in this Step: Gather Parameters for IHS and Plugin, continued

Parameter Name	Default Value	Required	Description
Location			same as the IHS Extract Location.
Install Manager Install Location	no default	required	Fully-qualified path where the Install Manager will be installed.
License Acceptance	false	required	Acknowledges that the end user agrees to the IBM International Program License Agreement. This is set to false by default and must be set to true for the installation to continue.
Web Server Name	no default	required	Required: Fully-qualified name of the Web server instance. There can be no spaces in the name. For example: `myapp.hp.com`
Web Service Password	no default	required	Password for the discovery web service API.
Web Service User	no default	required	User capable of modifying the managed environment through the discovery web service API.

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

See "Parameters for Provision IBM HTTP Server and Plug-in" for detailed descriptions of all input parameters for this workflow, including default values.

Tip: To avoid having to re-enter passwords whenever they change, you can create a policy to provide them to the workflow.

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

To verify the results:

Be sure to also perform the following step:

After the workflow has completed, run the following command to check the version of IBM HTTP Server that was installed:

WAS_ROOT/bin/versionInfo.sh

Here, *WAS_ROOT* is the directory where IBM HTTP Server was installed. For example: `/opt/IBM/HTTPServer`

Sample Scenario

This topic shows you typical parameter values used for the "Provision IBM HTTP Server and Plug-in" workflow.

Tip: To avoid having to re-enter passwords whenever they change, you can create a policy to provide them to the workflow.

Scenario 1:

Provision IBM HTTP Server 8 and plug-in with root - Parameter Value Examples

Parameter Name	Example Value	Description
Http Port	80	The port on which the Web server will listen. Default is set to 80. If the Web server instance is run as non-root this value has to be greater than 1024.
IHS Binary Download Location	`/opt/wasv8`	Name of the compressed IHS software package.
IHS Binary Files	`IHSbinary1.zip, IHSbinary2.zip, IHSbinary3.zip, IHSbinary4.zip,`	Name of the compressed IHS software package.
IHS Extract Location	`/opt/ihsv8`	Fully-qualified path where the compressed software will be extracted on the target machine. This cannot be the same as the Install Manager Extract Location.
IHS Install Location	`/opt/IBM/HTTPServer`	Fully-qualified path where IHS will be installed.
Install Manager Binary Download Location	`/opt/IBM/iim`	Fully-qualified path to the compressed Install Manager software package on the target machine.
Install Manager Binary Files	`IBM_Install_Manager_ Linux_1.5.3.zip`	Name of the compressed Install Manager software package.
Install Manager Extract Location	`/opt/IBM/iim`	Fully-qualified path where the compressed software will be extracted on the target machine. This location cannot be the same as the IHS Extract Location.
Install Manager Install Location	`/opt/IBM/ installManager`	Fully-qualified path where the Install Manager will be installed.
License Acceptance	true	Acknowledges that the end user agrees to the IBM International Program License Agreement. This is set to false by default and must be set to true for the installation to continue.

Provision IBM HTTP Server 8 and plug-in with root - Parameter Value Examples, continued

Parameter Name	Example Value	Description
Web Server Name	`example.mycompany.com`	Required: Fully-qualified name of the Web server instance. There can be no spaces in the name. For example: `myapp.hp.com`
Web Service Password	WebSrvPsWd	Password for the discovery web service API.
Web Service User	no default	User capable of modifying the managed environment through the discovery web service API.

Scenario 2:

Provision IBM HTTP Server 8 and plug-in with non-root - Parameter Value Examples

Parameter Name	Example Value	Description
Http Port	80	The port on which the Web server will listen. Default is set to 80. If the Web server instance is run as non-root this value has to be greater than 1024.
IHS Binary Download Location	`/opt/wasv8`	Name of the compressed IHS software package.
IHS Binary Files	`IHSbinary1.zip, IHSbinary2.zip, IHSbinary3.zip, IHSbinary4.zip,`	Name of the compressed IHS software package.
IHS Extract Location	`/opt/ihsv8`	Fully-qualified path where the compressed software will be extracted on the target machine. This cannot be the same as the Install Manager Extract Location.
IHS Install Location	`/opt/IBM/HTTPServer`	Fully-qualified path where IHS will be installed.
Install Manager Binary Download Location	`/opt/IBM/iim`	Fully-qualified path to the compressed Install Manager software package on the target machine.
Install Manager Binary Files	`IBM_Install_Manager_Linux_1.5.3.zip`	Name of the compressed Install Manager software package.

Provision IBM HTTP Server 8 and plug-in with non-root - Parameter Value Examples, continued

Parameter Name	Example Value	Description
Install Manager Extract Location	`/opt/IBM/iim`	Fully-qualified path where the compressed software will be extracted on the target machine. This location cannot be the same as the IHS Extract Location.
Install Manager Install Location	`/opt/IBM/installManager`	Fully-qualified path where the Install Manager will be installed.
License Acceptance	true	Acknowledges that the end user agrees to the IBM International Program License Agreement. This is set to false by default and must be set to true for the installation to continue.
Web Server Name	`example.mycompany.com`	Required: Fully-qualified name of the Web server instance. There can be no spaces in the name. For example: `myapp.hp.com`
Web Service Password	WebSrvPsWd	Password for the discovery web service API.
Web Service User	no default	User capable of modifying the managed environment through the discovery web service API.
IHS System Group	webadmin	The group that owns and runs the Web server instances and the plug-in directories. If the system group account does not already exist the account will be created on the target machine.
IHS System Password	SysPsWd	The password for the user that owns and runs the Web server instances and the plug-in directories. This password will be used when creating the system user.
IHS System User	ihsadmin	The user that owns and runs the Web server instances and the plug-in directories. If the system user account does not already exist the account will be created on the target machine.

Note: For this use case you need to expose the following parameters in the Gather Advanced Parameters for IHS and Plugin step:

The IHS System parameters: IHS System Group, IHS System Password, and IHS System User

Scenario 3:

Provision IBM HTTP Server 8, plug-in, and HTTP Admin Server with non-root - Parameter Value Examples

Parameter Name	Example Value	Description
Http Port	80	The port on which the Web server will listen. Default is set to 80. If the Web server instance is run as non-root this value has to be greater than 1024.
IHS Binary Download Location	`/opt/wasv8`	Name of the compressed IHS software package.
IHS Binary Files	`IHSbinary1.zip, IHSbinary2.zip, IHSbinary3.zip, IHSbinary4.zip,`	Name of the compressed IHS software package.
IHS Extract Location	`/opt/ihsv8`	Fully-qualified path where the compressed software will be extracted on the target machine. This cannot be the same as the Install Manager Extract Location.
IHS Install Location	`/opt/IBM/HTTPServer`	Fully-qualified path where IHS will be installed.
Install Manager Binary Download Location	`/opt/IBM/iim`	Fully-qualified path to the compressed Install Manager software package on the target machine.
Install Manager Binary Files	`IBM_Install_ Manager_Linux_ 1.5.3.zip`	Name of the compressed Install Manager software package.
Install Manager Extract Location	`/opt/IBM/iim`	Fully-qualified path where the compressed software will be extracted on the target machine. This location cannot be the same as the IHS Extract Location.
Install Manager Install Location	`/opt/IBM/ installManager`	Fully-qualified path where the Install Manager will be installed.
License Acceptance	true	Acknowledges that the end user agrees to the IBM International Program License Agreement. This is set to false by default and must be set to true for the installation to continue.
Web Server Name	`example. mycompany.com`	Required: Fully-qualified name of the Web server instance. There can be no spaces in the name. For example: `myapp.hp.com`

Provision IBM HTTP Server 8, plug-in, and HTTP Admin Server with non-root - Parameter Value Examples, continued

Parameter Name	Example Value	Description
Web Service Password	WebSrvPsWd	Password for the discovery web service API.
Web Service User	no default	User capable of modifying the managed environment through the discovery web service API.
HTTP Admin Password	AdMinPsWd	Password for the HTTP Admin User. If specified, HTTP Admin Port and HTTP Admin User must also be specified. If not specified, HTTP Admin Port and HTTP Admin User must not be specified.
HTTP Admin Port	8004	Port of the IBM HTTP Server administrative server. If specified, HTTP Admin Password and HTTP Admin User must also be specified. If not specified, HTTP Admin Password and HTTP Admin User must not be specified.
HTTP Admin User	wasadmin	User name of the IBM HTTP administrative user. If specified, HTTP Admin Password and HTTP Admin Port must also be specified. If not specified, HTTP Admin Password and HTTP Admin Port must not be specified.
IHS System Group	webadmin	The group that owns and runs the Web server instances and the plug-in directories. If the system group account does not already exist the account will be created on the target machine.
IHS System Password	SysPsWd	The password for the user that owns and runs the Web server instances and the plug-in directories. This password will be used when creating the system user.
IHS System User	ihsadmin	The user that owns and runs the Web server instances and the plug-in directories. If the system user account does not already exist the account will be created on the target machine.

Note: For this use case you need to expose the following parameters in the Gather Advanced Parameters for IHS and Plugin step:

- The IHS System parameters: IHS System Group, IHS System Password, and IHS System User
- The HTTP Admin parameters: HTTP Admin Password, HTTP Admin Port, and HTTP Admin User

Scenario 4:

Provision IBM HTTP Server 8, plug-in, HTTP Admin Server, and HTTP SSL with non-root - Parameter Value Examples

Parameter Name	Example Value	Description
Http Port	80	The port on which the Web server will listen. Default is set to 80. If the Web server instance is run as non-root this value has to be greater than 1024.
IHS Binary Download Location	`/opt/wasv8`	Name of the compressed IHS software package.
IHS Binary Files	`IHSbinary1.zip, IHSbinary2.zip, IHSbinary3.zip, IHSbinary4.zip,`	Name of the compressed IHS software package.
IHS Extract Location	`/opt/ihsv8`	Fully-qualified path where the compressed software will be extracted on the target machine. This cannot be the same as the Install Manager Extract Location.
IHS Install Location	`/opt/IBM/HTTPServer`	Fully-qualified path where IHS will be installed.
Install Manager Binary Download Location	`/opt/IBM/iim`	Fully-qualified path to the compressed Install Manager software package on the target machine.
Install Manager Binary Files	`IBM_Install_ Manager_Linux_ 1.5.3.zip`	Name of the compressed Install Manager software package.
Install Manager Extract Location	`/opt/IBM/iim`	Fully-qualified path where the compressed software will be extracted on the target machine. This location cannot be the same as the IHS Extract Location.
Install Manager Install Location	`/opt/IBM/ installManager`	Fully-qualified path where the Install Manager will be installed.
License Acceptance	true	Acknowledges that the end user agrees to the IBM International Program License Agreement. This is set to false by default and must be set to true for the installation to continue.
Web Server Name	`example. mycompany.com`	Required: Fully-qualified name of the Web server instance. There can be no spaces in the name. For example:

Provision IBM HTTP Server 8, plug-in, HTTP Admin Server, and HTTP SSL with non-root - Parameter Value Examples, continued

Parameter Name	Example Value	Description
		myapp.hp.com
Web Service Password	WebSrvPsWd	Password for the discovery web service API.
Web Service User	no default	User capable of modifying the managed environment through the discovery web service API.
HTTP Admin Password	AdMinPsWd	Password for the HTTP Admin User. If specified, HTTP Admin Port and HTTP Admin User must also be specified. If not specified, HTTP Admin Port and HTTP Admin User must not be specified.
HTTP Admin Port	8004	Port of the IBM HTTP Server administrative server. If specified, HTTP Admin Password and HTTP Admin User must also be specified. If not specified, HTTP Admin Password and HTTP Admin User must not be specified.
HTTP Admin User	wasadmin	User name of the IBM HTTP administrative user. If specified, HTTP Admin Password and HTTP Admin Port must also be specified. If not specified, HTTP Admin Password and HTTP Admin Port must not be specified.
HTTP SSL Port	443	The port on which the Web server will listen for SSL requests. Typically, this is set to 443. If the Web server instance is run as non-root this value has to be greater than 1024.
IHS System Group	webadmin	The group that owns and runs the Web server instances and the plug-in directories. If the system group account does not already exist the account will be created on the target machine.
IHS System Password	SysPsWd	The password for the user that owns and runs the Web server instances and the plug-in directories. This password will be used when creating the system user.
IHS System User	ihsadmin	The user that owns and runs the Web server instances and the plug-in directories. If the system user account does not already exist the account will be created on the target machine.
SSL Key Database Password	SslKeyDbPsWd	The password that will be used to create the SSL key database used to store the Web server instance SSL certificates.

Note: For this use case you need to expose the following parameters in the Gather Advanced Parameters for IHS and Plugin step:

- The IHS System parameters: IHS System Group, IHS System Password, and IHS System User
- The HTTP Admin parameters: HTTP Admin Password, HTTP Admin Port, and HTTP Admin User
- The SSL parameters: HTTP SSL Port and SSL Key Database Password

Parameters for Provision IBM HTTP Server and Plug-in

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

Input Parameters Defined in this Step: Gather Parameters for IHS and Plugin

Parameter Name	Default Value	Required	Description
Http Port	80	required	The port on which the Web server will listen. Default is set to 80. If the Web server instance is run as non-root this value has to be greater than 1024.
IHS Binary Download Location	no default	required	Name of the compressed IHS software package.
IHS Binary Files	no default	required	Name of the compressed IHS software package.
IHS Extract Location	no default	required	Fully-qualified path where the compressed software will be extracted on the target machine. This cannot be the same as the Install Manager Extract Location.
IHS Install Location	no default	required	Fully-qualified path where IHS will be installed.
Install Manager Binary Download Location	no default	required	Fully-qualified path to the compressed Install Manager software package on the target machine.
Install Manager Binary Files	no default	required	Name of the compressed Install Manager software package.
Install Manager Extract Location	no default	required	Fully-qualified path where the compressed software will be extracted on the target machine. This location cannot be the same as the IHS Extract Location.
Install Manager Install Location	no default	required	Fully-qualified path where the Install Manager will be installed.
License Acceptance	false	required	Acknowledges that the end user agrees to the IBM International Program License Agreement. This is set to false by default and must be set to true for the installation to continue.
Web Server Name	no default	required	Required: Fully-qualified name of the Web server instance. There can be no spaces in the name. For example: `myapp.hp.com`
Web Service Password	no default	required	Password for the discovery web service API.

Input Parameters Defined in this Step: Gather Parameters for IHS and Plugin, continued

Parameter Name	Default Value	Required	Description
Web Service User	no default	required	User capable of modifying the managed environment through the discovery web service API.

Additional Input Parameters Defined in this Step: Gather Advanced Parameters for IHS and Plugin

Parameter Name	Default Value	Required	Description
Access Log File	see description	optional	Fully-qualified path for the IBM HTTP Server access log file. For example: `/opt/IBM/HTTPServer/logs` The default is based on the values of IHS Install Location and Web Server Name.
Cleanup on Failure	True	optional	Indicates whether to remove downloaded and extracted files and to clean up the installation directory in the event of workflow failure. Valid values are True and False. The default is True, which will clean up on failure.
Cleanup on Success	True	optional	Indicates whether to remove downloaded and extracted files and to clean up the installation directory in the event of workflow success. Valid values are True and False. The default is True, which will clean up on success.
Error Log File	see description	optional	Fully-qualified path for the IBM HTTP Server error log file. For example: `/opt/IBM/HTTPServer/logs` The default is based on the values of IHS Install Location and Web Server Name.
HTTP Admin Password	no default	optional	Password for the HTTP Admin User. If specified, HTTP Admin Port and HTTP Admin User must also be specified. If not specified, HTTP Admin Port and HTTP Admin User must not be specified.
HTTP Admin Port	no default	optional	Port of the IBM HTTP Server administrative server. If specified, HTTP Admin Password and HTTP Admin User must also be specified. If not specified, HTTP Admin Password and HTTP Admin User must not be specified.
HTTP Admin User	no default	optional	User name of the IBM HTTP administrative user. If specified, HTTP Admin Password and HTTP Admin Port must also be specified. If not specified, HTTP Admin Password and HTTP Admin Port must not be

Additional Input Parameters Defined in this Step: Gather Advanced Parameters for IHS and Plugin, continued

Parameter Name	Default Value	Required	Description
			specified.
HTTP Configuration File	see description	optional	Fully-qualified path for the IBM HTTP Server configuration file. For example: `/opt/IBM/HTTPServer/conf/httpd.conf` The default is based on the values of IHS Install Location and Web Server Name.
HTTP SSL Port	no default	optional	The port on which the Web server will listen for SSL requests. Typically, this is set to 443. If the Web server instance is run as non-root this value has to be greater than 1024.
IHS System Group	no default	optional	The group that owns and runs the Web server instances and the plug-in directories. If the system group account does not already exist the account will be created on the target machine.
IHS System Password	no default	optional	The password for the user that owns and runs the Web server instances and the plug-in directories. This password will be used when creating the system user.
IHS System User	no default	optional	The user that owns and runs the Web server instances and the plug-in directories. If the system user account does not already exist the account will be created on the target machine.
IPaddr	see description	optional	IP address that binds the Web server to a specific IP address and ports. The default value is the IP address of `${Server.Name}`.
Plugin Install Root	see description	optional	Fully-qualified path where the WebSphere plug-in is installed. The default is based on IHS Install Location.
Response File	see description	optional	Fully-qualified path where the response file that this workflow creates will be located. This file is used to drive the installation. The default is `/tmp/installrespFile.xml`
SSL Key Database Password	no default	optional	The password that will be used to create the SSL key database used to store the Web server instance SSL certificates.

Provision WebSphere 7 and Custom Node

Use this workflow to install the WebSphere 7 Base core binaries and, optionally, create a custom profile.

A custom profile initially contains an empty node with no servers. The workflow can add (federate) the server to the pertinent cell when the profile is created, or you can add it later yourself.

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

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

Prerequisites for this Workflow

Be sure that the following prerequisites are satisfied before you run the Provision WebSphere 7 and Custom Node workflow:

1. This workflow requires unchallenged `sudo` access to a user (typically root) who can access all required files and directories.
2. Per the WebSphere 7 documentation, the following system libraries are required before provisioning IBM WebSphere Application Server version 7 on 64-bit Red Hat Linux:

Platform	Required Library
64-bit Red Hat Enterprise Linux version 5	compat-libstdc++-33-3.2.3-61 compat-db-4.2.52-5.1 libXp-1.0.0-8 compat-libstdc++- 296-2.96-138 rpm-build- 4.4.2-37.el5

   Make sure that these libraries exist on each target server before running this workflow. If newer versions of these libraries are available, you can install the newer versions.
3. This workflow will install WebSphere Application Server as root because of the following IBM documented limitations:
   - Creation of a Linux service for WebSphere Application Server
   - Native registration with the operating system
   - Port conflicts that may occur with other installations of WebSphere Application Server that are not registered with the operating system

   If there is a need to run as a non-root user after installation, you can run a recursive `chown` under the installation root and set owner permissions accordingly.

For more information about prerequisites for WebSphere 7, refer to the WebSphere 8 Product Documentation.

How this Workflow Works

This topic contains the following information about the Provision WebSphere 7 and Custom Node workflow:

Overview

This workflow does the following things in the order shown:

1. Prepares and validates all parameters and creates the call wrapper that will be used to execute commands within a WebSphere 7 environment
2. Checks the documented library requirements, files system space requirements, and temporary space requirements
3. Checks whether the WebSphere 7 binaries are available—if not, they will be downloaded from the software repository—and extracts the binary files from the compressed archive
4. Creates a new response file
5. Provisions IBM WebSphere Application Server version 7 on a target machine
6. Creates a custom node profile
7. Optionally federates the custom managed node profile into a Deployment Manager

Validation Checks Performed

Most of the validation centers on special characters and spaces in the parameters. There are also validation checks that happen at the operating system level, including file system space checks and RPM checks for Red Hat Linux.

The workflow first performs the following parameter checks:

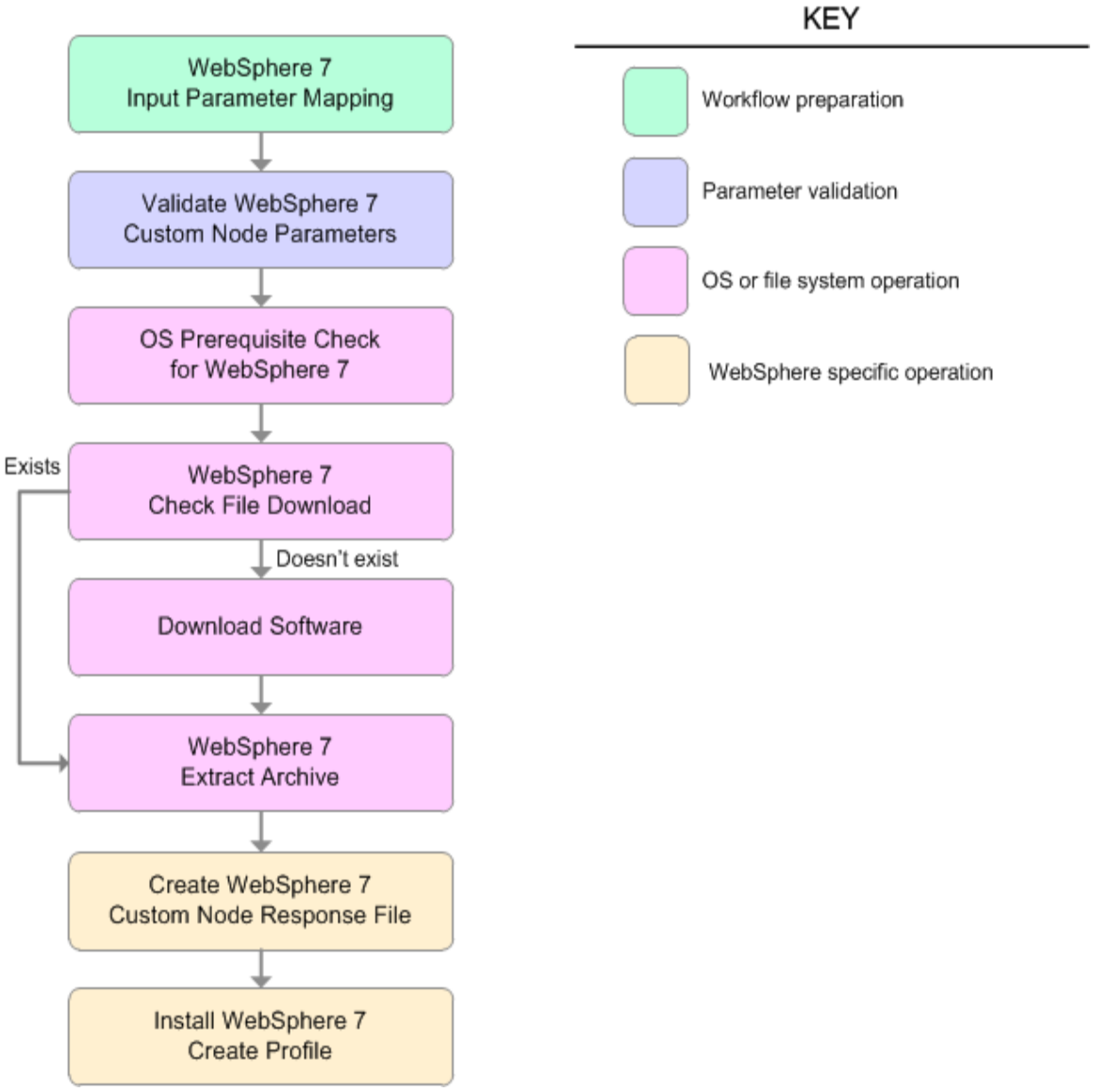
1. Enable Security is true or false. If Enable Security is true, Admin Password and Admin User are specified.
2. Admin User (if specified) does not begin with a period (.), hyphen (-) or space. It does not contain any of the following characters: / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }
3. Admin Password (if specified) does not begin with a hyphen (-) or contain a space.
4. Cell Name, Node Name, and Profile Name are specified. They do not contain the following characters: / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { } or space. They do not begin with a period.
5. Host Name is specified.
6. Ports File (if specified) exists.
7. Federate Later (if specified) is true or false.
8. Dmgr HostName is specified.
9. Dmgr Port (if specified) is an integer.
10. License Acceptance is true.
11. Binary Archive is specified. It either exists or can be created successfully.
12. Extract Path and Install Location either exist or can be created successfully.
13. Profile Path and Response File are specified.
14. Profile Type is custom.

The workflow then performs the following operating system checks on the target machine:

1. All required libraries are present (see "Prerequisites for this Workflow" on page 113).
2. Sufficient disk space is available to install WebSphere 7.
3. Sufficient disk space is available to extract the binary files from the compressed archive.

Steps Executed

The Provision WebSphere 7 and Custom Node workflow includes the following steps. Each step must complete successfully before the next step can start. If a step fails, the workflow reports a failure, and all subsequent steps are skipped.



Steps Used in the Provision WebSphere 7 and Custom Node Workflow

Workflow Step	Description
WebSphere 7 Input Parameter Mapping	This step creates the call wrapper—the command that executes the step as a specific user—and allows certain parameters to be hidden or exposed.
Validate WebSphere 7 Custom Node Parameters	This step prepares and validates the parameters needed to install WebSphere Application Server V7.0 and create a custom node profile.
OS Prerequisite Check for WebSphere 7	This step checks the documented library requirements, files system space requirements, and temporary space requirements for WebSphere Application Server V7.0.
WebSphere 7 Check File Download	This step checks for the existence of a file before downloading it from the software repository: • Checks if a file exists in the expected location. • If the file is not in the expected location, the file is added to a list of files that need to be downloaded.
Download Software	This step downloads a list of files to a specified location on the target server.
WebSphere 7 Extract Archive	This step checks that the archive file exists

Steps Used in the Provision WebSphere 7 and Custom Node Workflow, continued

Workflow Step	Description
	and then, based on the archive extension, extracts the archive to the specified directory.
Create WebSphere 7 Custom Node Response File	This step creates a new response file for installing a new instance of WebSphere Application Server V7.0 and creating a custom node profile.
Install WebSphere 7 Create Profile	This step installs a new instance of WebSphere Application Server V7.0 using the `install -options <responsefile> silent` option and then creates a profile.

For parameter descriptions and defaults, see "Parameters for Provision WebSphere 7 and Custom Node" on page 124.

How to Run this Workflow

The following instructions show you how to customize and run the Provision WebSphere 7 and Custom Node workflow in your environment.

The workflow provides default values for some parameters. These default values are usually sufficient for a "typical" installation. You can override the defaults by specifying parameter values in the deployment. You can also expose additional parameters in the workflow, if necessary, to accomplish more advanced scenarios. Any parameters not explicitly specified in the deployment will have the default values listed in "Parameters for Provision WebSphere 7 and Custom Node" on page 124.

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

To customize and run the Provision WebSphere 7 and Custom Node workflow:

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

Input Parameters for Validate WebSphere 7 Custom Node Parameters

Parameter Name	Default Value	Required	Description
Binary Archive	no default	required	Fully qualified path to the compressed software package on the target machine. For example: `/opt/install/C1G36ML.tar.gz`
Cell Name	no default	required	Unique cell name that does not contain any of the following special characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }. If you plan to federate into an existing cell later, make sure that this name is not the same as the existing cell name.
Dmgr Admin Password	no default	optional	Administrative user password for the Deployment Manager. When Enable Security is set to true, this parameter must contain a string that does not begin with a dash(-) or contain a space( ).
Dmgr Admin User	no default	optional	Deployment Manager administrative user. When Enable Security is set to true, this parameter must contain a string that does not begin with a dash(-), a period(.), or a space( ). It cannot contain any of the following characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }.
Dmgr HostName	no default	optional	Host name or IP address of the machine where the Deployment Manager is running. Specify this parameter and the Dmgr Port parameter to federate the new custom node as it is created. If you do not specify a value for this parameter, the new custom node is not federated (you must federate it later). Required if Federate Later is set to false.

Input Parameters for Validate WebSphere 7 Custom Node Parameters, continued

Parameter Name	Default Value	Required	Description
Dmgr Port	no default	optional	The SOAP port on which the Deployment Manager is listening. Specify this parameter and the Dmgr Host Name parameter to federate the new custom node as it is created. If you do not specify a value for this parameter, the new custom node is not federated (you must federate it later). Required if Federate Later is set to false.
Enable Security	no default	required	Enables administrative security on the Deployment Manager. Must be set to either true or false. If Enable Security is true, the Dmgr Admin User and Dmgr Admin Password parameters must have values.
Extract Dir	no default	required	Fully qualified path where the compressed software will be extracted on the target machine.
Federate Later	no default	required	If false, the new custom node will be federated by the workflow during profile creation. If true, you must federate it later manually by using the addNode command.
Install Location	no default	required	Fully qualified path where WebSphere Application Server will be installed. For example: `/opt/IBM/WebSphere/AppServer`
License Acceptance	false	required	Acknowledges that the end user agrees to the IBM International Program License Agreement. This is set to false by default and must be set to true in order for the installation to continue.
Node Name	no default	required	Unique node name that cannot contain any of the following special characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }. If you plan to federate into an existing cell later, make sure that the name is unique within that cell.
Profile Name	no default	required	A unique profile name. It cannot begin with a period (.) and cannot contain any of the following special characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }.
Profile Path	no default	required	Fully qualifed path to the custom node profile. For example: `/opt/IBM/WebSphere/AppServer/profiles/ProdNode01`
Profile Type	custom	required	Because this workflow creates a Custom Node profile, the value must be custom.
Response File	no default	required	Fully qualified path where the response file that this workflow creates will be located. This file will then be used to drive the installation and profile creation.

Additional Input Parameters for Install WebSphere 7 Create Profile

Parameter Name	Default Value	Required	Description
Password	no default	required	The Windows Administrator password. Required for Windows.
Username	no default	required	This is the Windows Administrator user. Required for Windows.

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

See "Parameters for Provision WebSphere 7 and Custom Node" on page 124 for detailed descriptions of all input parameters for this workflow, including default values.

Tip: To avoid having to re-enter passwords whenever they change, you can create a policy to provide them to the workflow.

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

To verify the results:

Optional: if you want to further verify the results, perform the following steps:

1. After the workflow has completed, run the following command to check the version of WebSphere Application Server that was installed:

   WAS_ROOT/bin/versionInfo.sh

   Here, *WAS_ROOT* is the directory where WebSphere 7 is installed. This is the path that you specified in the WebSphere Install Location parameter.
2. Validate that the Deployment Manager profile has been created and is running by doing the following:
   a. View the *WAS_ROOT*/profiles/*PROFILE_NAME*/logs/AboutThisProfile.txt file. This file is created after the creation of the profile and contains specific information about the profile.

      Here, *PROFILE_NAME* is the name of the profile that you just created. This is the name that you specified in the Profile Name parameter.

   b. Change to the *WAS_ROOT*/profiles/*PROFILE_NAME*/logs/nodeagent directory, and tail the SystemOut.log file. Look for the following line:

      Server nodeagent open for e-business

Sample Scenario

This topic shows you typical parameter values used for the Provision WebSphere 7 and Custom Node workflow.

New WebSphere 7 install with custom node profile

Input Parameters for Validate WebSphere 7 Custom Node Parameters

Parameter Name	Example Value	Description
Binary Archive	see description	Fully qualified path to the compressed software package on the target machine. For example: `/opt/install/C1G36ML.tar.gz`
Cell Name	Dev NodeCell	Unique cell name that does not contain any of the following special characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }. If you plan to federate into an existing cell later, make sure that this name is not the same as the existing cell name.
Dmgr Admin Password	wasPassWord	Administrative user password for the Deployment Manager. When Enable Security is set to true, this parameter must contain a string that does not begin with a dash(-) or contain a space( ).
Dmgr Admin User	wasadmin	Deployment Manager administrative user. When Enable Security is set to true, this parameter must contain a string that does not begin with a dash(-), a period(.), or a space( ). It cannot contain any of the following characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }.
Dmgr HostName	mycompany.com	Host name or IP address of the machine where the Deployment Manager is running. Specify this parameter and the Dmgr Port parameter to federate the new custom node as it is created. If you do not specify a value for this parameter, the new custom node is not federated (you must federate it later). Required if Federate Later is set to false.
Dmgr Port	8879	The SOAP port on which the Deployment Manager is listening. Specify this parameter and the Dmgr Host Name parameter to federate the new custom node as it is created. If you do not specify a value for this parameter, the new custom node is not federated (you must federate it later). Required if Federate Later is set to false.
Enable Security	true	Enables administrative security on the Deployment Manager. Must be set to either true or false. If Enable Security is true, the Dmgr Admin User and Dmgr Admin Password parameters must have values.
Extract Dir	`/opt/IBM/wasv7`	Fully qualified path where the compressed software will be extracted on the target machine.
Federate Later	true	If false, the new custom node will be federated by the workflow during profile creation; you must specify Dmgr HostName and Dmgr Port to do this. If true, you must federate it later manually by using the addNode command.

Input Parameters for Validate WebSphere 7 Custom Node Parameters, continued

Parameter Name	Example Value	Description
Install Location	see description	Fully qualified path where WebSphere Application Server will be installed. For example: `/opt/IBM/WebSphere/AppServer`
License Acceptance	true	Acknowledges that the end user agrees to the IBM International Program License Agreement. This is set to false by default and must be set to true in order for the installation to continue.
Node Name	DevNode	Unique node name that cannot contain any of the following special characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }. If you plan to federate into an existing cell later, make sure that the name is unique within that cell.
Profile Name	DevNode	A unique profile name. It cannot begin with a period (.) and cannot contain any of the following special characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }.
Profile Path	see description	Fully qualifed path to the custom node profile. For example: `/opt/IBM/WebSphere/AppServer/profiles/ProdNode01`
Profile Type	custom	Because this workflow creates a Custom Node profile, the value must be custom.
Response File	`/tmp/serverrsp`	Fully qualified path where the response file that this workflow creates will be located. This file will then be used to drive the installation and profile creation.

Tip: To avoid having to re-enter passwords whenever they change, you can create a policy to provide them to the workflow.

Parameters for Provision WebSphere 7 and Custom Node

Tip: To avoid having to re-enter passwords whenever they change, you can create a policy to provide them to the workflow.

Note: Only those parameters that are configurable in a standard deployment are listed here. Input parameters that must be mapped to output parameters of previous steps are not listed.

Parameters Defined in this Step: Validate WebSphere 7 Custom Node Parameters

Parameter Name	Default Value	Required	Description
Binary Archive	no default	required	Fully qualified path to the compressed software package on the target machine. For example: `/opt/install/C1G36ML.tar.gz`
Call Wrapper	see description	required	Command that will execute this step (or subsequent steps) as a specific user. For UNIX targets, the default is: `/opt/hp/dma/client/jython.sh` running as root For Windows targets, the default is: `jython` running as Administrator This parameter is derived by the workflow. Under most circumstances, you should not change its mapping or its value.
Cell Name	no default	required	Unique cell name that does not contain any of the following special characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }. If you plan to federate into an existing cell later, make sure that this name is not the same as the existing cell name.
Dmgr Admin Password	no default	optional	Administrative user password for the Deployment Manager. When Enable Security is set to true, this parameter must contain a string that does not begin with a dash(-) or contain a space( ).
Dmgr Admin User	no default	optional	Deployment Manager administrative user. When Enable Security is set to true, this parameter must contain a string that does not begin with a dash(-), a period(.), or a space( ). It cannot contain any of the following characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }.
Dmgr HostName	no default	optional	Host name or IP address of the machine where the Deployment Manager is running. Specify this parameter and the Dmgr Port parameter to federate the new custom node as it is created. If you do not specify a value for this parameter, the new custom node is not

Parameters Defined in this Step: Validate WebSphere 7 Custom Node Parameters, continued

Parameter Name	Default Value	Required	Description
			federated (you must federate it later). Required if Federate Later is set to false.
Dmgr Port	no default	optional	The SOAP port on which the Deployment Manager is listening. Specify this parameter and the Dmgr Host Name parameter to federate the new custom node as it is created. If you do not specify a value for this parameter, the new custom node is not federated (you must federate it later). Required if Federate Later is set to false.
Enable Security	no default	required	Enables administrative security on the Deployment Manager. Must be set to either true or false. If Enable Security is true, the Dmgr Admin User and Dmgr Admin Password parameters must have values.
Extract Dir	no default	required	Fully qualified path where the compressed software will be extracted on the target machine.
Federate Later	no default	required	If false, the new custom node will be federated by the workflow during profile creation. If true, you must federate it later manually by using the addNode command.
Host Name	Server.name	required	Hostname or IP address of the target machine.
Install Location	no default	required	Fully qualified path where WebSphere Application Server will be installed. For example: `/opt/IBM/WebSphere/AppServer`
Keystore Password	no default	required	Sets the password for all keystore files created during profile creation. This includes keystore files for both the default personal certificate and the root signing certificate.
License Acceptance	false	required	Acknowledges that the end user agrees to the IBM International Program License Agreement. This is set to false by default and must be set to true in order for the installation to continue.
Node Name	no default	required	Unique node name that cannot contain any of the following special characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }. If you plan to federate into an existing cell later, make sure that the name is unique within that cell.
Personal CertDN	no default	optional	Distinguished name of the personal certificate. For example: CN=dmalab-example.com,OU=WAS7LabCell, OU=WAS7LabDmgrManager,O=IBM,C=US

Parameters Defined in this Step: Validate WebSphere 7 Custom Node Parameters, continued

Parameter Name	Default Value	Required	Description
			The DN string cannot contain spaces. If you do not specify the DN, the WebSphere Application Server installer will create one.
Personal CertValidity Period	1	optional	Amount of time in years that the personal certificate is valid. Default is one year.
Ports File	no default	optional	Fully qualified path to a file that defines port settings for the new profile. This file must contain key=value pairs that specify a service name and a port number (for example: WC_adminhost=9060). This option should be used with the Validate Ports option.
Profile Name	no default	required	A unique profile name. It cannot begin with a period (.) and cannot contain any of the following special characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }.
Profile Path	no default	required	Fully qualifed path to the custom node profile. For example: `/opt/IBM/WebSphere/AppServer/profiles/ProdNode01`
Profile Type	no default	required	Because this workflow creates a Custom Node profile, the value must be custom.
Response File	no default	required	Fully qualified path where the response file that this workflow creates will be located. This file will then be used to drive the installation and profile creation.
Signing CertDN	no default	optional	Distinguished name of the signing certificate. For example: CN=dmalab-example.com, OU=Root Certificate, OU=WAS7TestLabCell, OU=WAS7LabNode1, O=IBM, C=US The DN string cannot contain spaces. If you do not specify the DN, the WebSphere Application Server installer will create one.
Signing CertValidity Period	15	optional	Amount of time in years that the root certificate is valid. Default is 15 years.

Additional Parameters Defined in this Step: Install WebSphere 7 Create Profile

Parameter Name	Default Value	Required	Description
Password	no default	required	The Windows Administrator password. Required for Windows.

Additional Parameters Defined in this Step: Install WebSphere 7 Create Profile, continued

Parameter Name	Default Value	Required	Description
Username	no default	required	This is the Windows Administrator user. Required for Windows.

Provision WebSphere 7 and Deployment Manager

Use this workflow to install the WebSphere 7 Base core binaries and, optionally, create a Deployment Manager profile.

A Deployment Manager is the administration point for a cell that contains multiple application servers. This type of profile is appropriate for distributed application server environments.

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

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

Prerequisites for this Workflow

Be sure that the following prerequisites are satisfied before you run the Provision WebSphere 7 and Deployment Manager workflow:

1. This workflow requires unchallenged `sudo` access to a user (typically root) who can access all required files and directories.
2. Per the WebSphere 7 documentation, the following system libraries are required before provisioning IBM WebSphere Application Server version 7 on 64-bit Red Hat Linux:

Platform	Required Library
64-bit Red Hat Enterprise Linux version 5	compat-libstdc++-33-3.2.3-61 compat-db-4.2.52-5.1 libXp-1.0.0-8 compat-libstdc++- 296-2.96-138 rpm-build- 4.4.2-37.el5

   Make sure that these libraries exist on each target server before running this workflow. If newer versions of these libraries are available, you can install the newer versions.
3. This workflow will install WebSphere Application Server as root because of the following IBM documented limitations:
   - Creation of a Linux service for WebSphere Application Server
   - Native registration with the operating system
   - Port conflicts that may occur with other installations of WebSphere Application Server that are not registered with the operating system

   If there is a need to run as a non-root user after installation, you can run a recursive `chown` under the installation root and set owner permissions accordingly.

For more information about prerequisites for WebSphere 7, refer to the WebSphere 8 Product Documentation.

How this Workflow Works

This topic contains the following information about the Provision WebSphere 7 and Deployment Manager workflow:

Overview

This workflow does the following things in the order shown:

1. Prepares and validates all parameters and creates the call wrapper that will be used to execute commands within a WebSphere 7 environment
2. Checks the documented library requirements, files system space requirements, and temporary space requirements
3. Checks whether the WebSphere 7 binaries are available—if not, they will be downloaded from the software repository—and extracts the binary files from the compressed archive
4. Creates a new response file
5. Provisions IBM WebSphere Application Server version 7 on a target machine
6. Creates a Deployment Manager profile
7. Starts the WebSphere 7 Deployment Manager application server

Validation Checks Performed

Most of the validation centers on special characters and spaces in the parameters. There are also validation checks that happen at the operating system level, including file system space checks and RPM checks for Red Hat Linux.

The workflow first performs the following parameter checks:

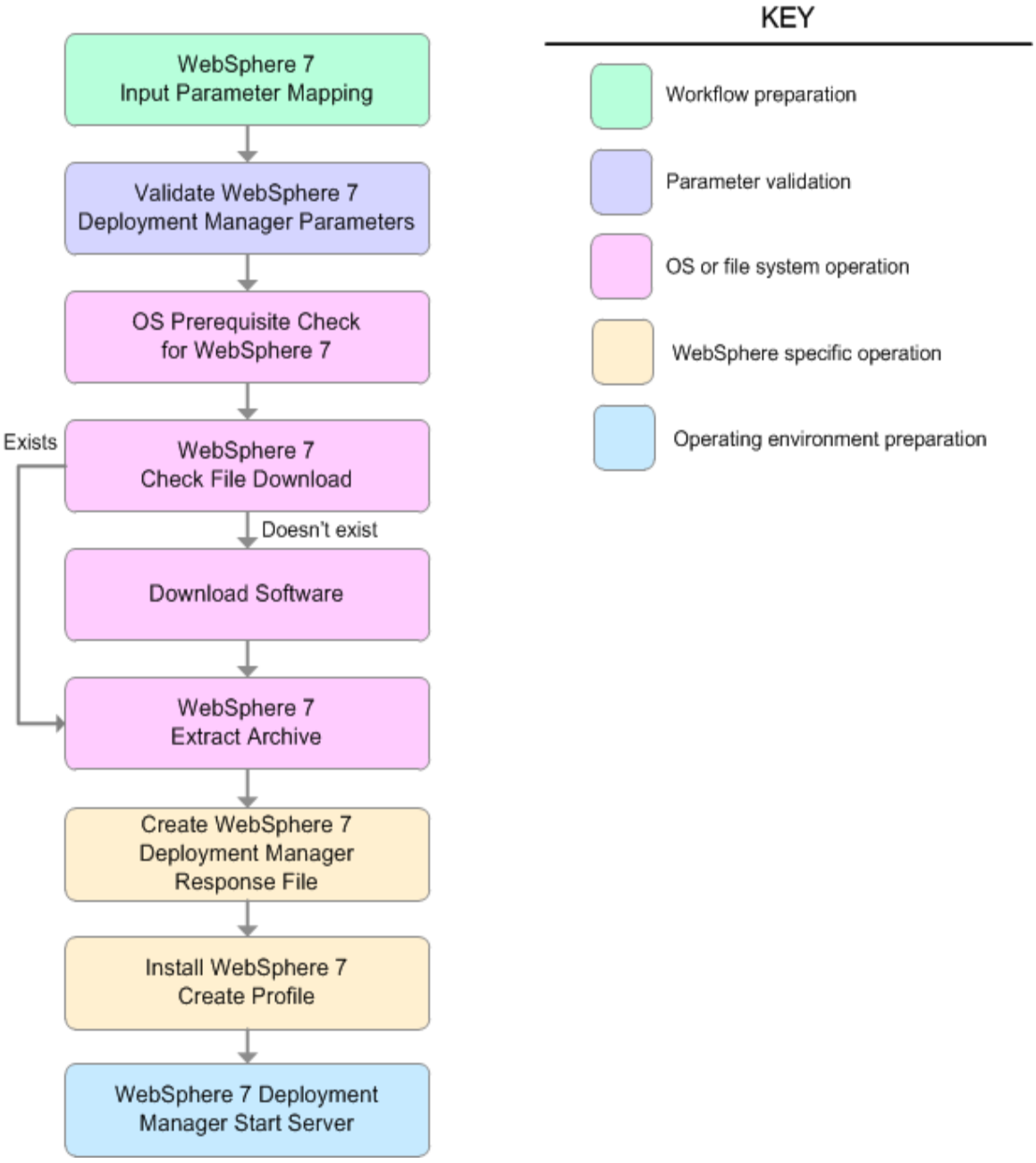
1. Admin User (if specified) does not begin with a period (.), hyphen (-) or space. It does not contain any of the following characters: / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }
2. Admin Password (if specified) does not begin with a hyphen (-) or contain a space.
3. Cell Name, Node Name, and Profile Name are specified. They do not contain the following characters: / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { } or space. They do not begin with a period.
4. Host Name is specified.
5. Default Ports (if specified) is true or false.
6. Enable Security is true or false. If Enable Security is true, Admin Password and Admin User are specified.
7. Omit Action (if specified) is defaultAppDeployAndConfig, or deployAdminConsole.
8. Ports File (if specified) exists and Validate Ports is true or false.
9. Starting Port (if specified) is an integer.
10. If the operating system is Windows, Windows Admin User and Windows Admin Password are specified.
11. License Acceptance is true.
12. Binary Archive is specified. It either exists or can be created successfully.
13. Extract Path and Install Location either exist or can be created successfully.
14. Profile Path and Response File are specified.
15. Server Type is DEPLOYMENT_MANAGER.
16. Profile Type is management.

The workflow then performs the following operating system checks on the target machine:

1. All required libraries are present (see "Prerequisites for this Workflow" on page 129).
2. Sufficient disk space is available to install WebSphere 7.
3. Sufficient disk space is available to extract the binary files from the compressed archive.

Steps Executed

The Provision WebSphere 7 and Deployment Manager workflow includes the following steps. Each step must complete successfully before the next step can start. If a step fails, the workflow reports a failure, and all subsequent steps are skipped.



Steps Used in the Provision WebSphere 7 and Deployment Manager Workflow

Workflow Step	Description
WebSphere 7 Input Parameter Mapping	This step creates the call wrapper—the command that executes the step as a specific user—and allows certain parameters to be hidden or exposed.
Validate WebSphere 7 Deployment Manager Parameters	This step prepares and validates the parameters needed to install WebSphere Application Server V7.0 and create a Deployment Manager profile.
OS Prerequisite Check for WebSphere 7	This step checks the documented library requirements, files system space requirements, and temporary space requirements for WebSphere Application Server V7.0.
WebSphere 7 Check File Download	This step checks for the existence of a file before downloading it from the software repository: • Checks if a file exists in the expected location. • If the file is not in the expected location, the file is added to a list of files that need to be downloaded.
Download Software	This step downloads a list of files to a specified location on the target server.
WebSphere 7 Extract Archive	This step checks that the archive file exists and then, based on the archive extension, extracts the archive to the specified directory.
Create WebSphere 7 Deployment Manager Response File	This step creates a new response file for installing a new instance of WebSphere Application Server V7.0 and creating a Deployment Manager profile.
Install WebSphere 7 Create Profile	This step installs a new instance of WebSphere Application Server V7.0 using the `install -options <responsefile> silent` option and then creates a profile.

Steps Used in the Provision WebSphere 7 and Deployment Manager Workflow, continued

Workflow Step	Description
WebSphere 7 Deployment Manager Start Server	This step starts the WebSphere 7 Deployment Manager application server.

For parameter descriptions and defaults, see "Parameters for Provision WebSphere 7 and Deployment Manager" on page 140.

How to Run this Workflow

The following instructions show you how to customize and run the Provision WebSphere 7 and Deployment Manager workflow in your environment.

The workflow provides default values for some parameters. These default values are usually sufficient for a "typical" installation. You can override the defaults by specifying parameter values in the deployment. You can also expose additional parameters in the workflow, if necessary, to accomplish more advanced scenarios. Any parameters not explicitly specified in the deployment will have the default values listed in "Parameters for Provision WebSphere 7 and Deployment Manager" on page 140.

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

To customize and run the Provision WebSphere 7 and Deployment Manager workflow:

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

Input Parameters for Validate WebSphere 7 Deployment Manager Parameters

Parameter Name	Default Value	Required	Description
Admin Password	no default	optional	When Enable Security is set to true, this parameter must contain a string that does not begin with a dash(-) or contain a space( ).
Admin User	no default	optional	When Enable Security is set to true, this parameter must contain a string that does not begin with a dash (-), a period(.), or a space( ). It cannot contain any of the following characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }.
Binary Archive	no default	required	Fully qualified path to the compressed software package on the target machine. For example: `/opt/install/C1G36ML.tar.gz`
Cell Name	no default	required	Unique cell name that does not contain any of the following special characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }. If you plan to federate into an existing cell later, make sure that this name is not the same as the existing cell name.
Enable Security	no default	required	Enables administrative security. Must be set to either true or false. If Enable Security is true, the Admin User and Admin Password parameters must have values.
Extract Dir	no default	required	Fully qualified path where the compressed software will be extracted on the target machine.
Install	no default	required	Fully qualified path where WebSphere Application

Input Parameters for Validate WebSphere 7 Deployment Manager Parameters, continued

Parameter Name	Default Value	Required	Description
Location			Server will be installed. For example: `/opt/IBM/WebSphere/AppServer`
License Acceptance	false	required	Acknowledges that the end user agrees to the IBM International Program License Agreement. This is set to false by default and must be set to true in order for the installation to continue.
Node Name	no default	required	Unique node name that cannot contain any of the following special characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }. If you plan to federate into an existing cell later, make sure that the name is unique within that cell.
Profile Name	no default	required	A unique profile name. It cannot begin with a period (.) and cannot contain any of the following special characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }.
Profile Path	no default	required	Fully qualifed path to the Deployment Manager profile. For example: `/opt/IBM/WebSphere/AppServer/profiles/ProdDmgr`
Profile Type	management	required	Because this workflow creates a Deployment Manager profile, the value must be management.
Response File	no default	required	Fully qualified path where the response file that this workflow creates will be located. This file will then be used to drive the installation and profile creation.
Server Type	DEPLOYMENT_MANAGER	required	The type of management profile. The value is DEPLOYMENT_MANAGER for a deployment manager server.
Windows Admin Password	no default	required	The Windows Administrator password. Required for Windows.
Windows Admin User	no default	required	This is the Windows Administrator user. Required for Windows.

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

See "Parameters for Provision WebSphere 7 and Deployment Manager" on page 140 for detailed descriptions of all input parameters for this workflow, including default values.

> **Tip:** To avoid having to re-enter passwords whenever they change, you can create a policy to provide them to the workflow.

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

To verify the results:

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

Optional: if you want to further verify the results, perform the following steps:

1. After the workflow has completed, run the following command to check the version of WebSphere Application Server that was installed:

   WAS_ROOT/bin/versionInfo.sh

   Here, *WAS_ROOT* is the directory where WebSphere 7 is installed. This is the path that you specified in the WebSphere Install Location parameter.
2. Validate that the Deployment Manager profile has been created and is running by doing the following:
   a. View the *WAS_ROOT*/profiles/*PROFILE_NAME*/logs/AboutThisProfile.txt file. This file is created after the creation of the profile and contains specific information about the profile.

      Here, *PROFILE_NAME* is the name of the profile that you just created. This is the name that you specified in the Profile Name parameter.

   b. Change to the *WAS_ROOT*/profiles/*PROFILE_NAME*/logs/dmgr directory, and tail the SystemOut.log file. Look for the following line:

      Server dmgr open for e-business

Sample Scenario

This topic shows you typical parameter values used for the Provision WebSphere 7 and Deployment Manager workflow.

New WebSphere 7 install with Deployment Manager profile

Input Parameters for Validate WebSphere 7 Deployment Manager Parameters

Parameter Name	Example Value	Description
Admin Password	wasPassWord	When Enable Security is set to true, this parameter must contain a string that does not begin with a dash(-) or contain a space( ).
Admin User	wasadmin	When Enable Security is set to true, this parameter must contain a string that does not begin with a dash(-), a period(.), or a space( ). It cannot contain any of the following characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }.
Binary Archive	see description	Fully qualified path to the compressed software package on the target machine. For example: `/opt/install/C1G36ML.tar.gz`
Cell Name	DevCell	Unique cell name that does not contain any of the following special characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }. If you plan to federate into an existing cell later, make sure that this name is not the same as the existing cell name.
Enable Security	true	Enables administrative security. Must be set to either true or false. If Enable Security is true, the Admin User and Admin Password parameters must have values.
Extract Dir	`/opt/IBM/wasv7`	Fully qualified path where the compressed software will be extracted on the target machine.
Install Location	see description	Fully qualified path where WebSphere Application Server will be installed. For example: `/opt/IBM/WebSphere/AppServer`
License Acceptance	true	Acknowledges that the end user agrees to the IBM International Program License Agreement. This is set to false by default and must be set to true in order for the installation to continue.
Node Name	no default	Unique node name that cannot contain any of the following special characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }. If you plan to federate into an existing cell later, make sure that the name is unique within that cell.
Profile Name	no default	A unique profile name. It cannot begin with a period (.) and cannot contain any of the following special characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }.
Profile Path	no default	Fully qualifed path to the Deployment Manager profile. For example: `/opt/IBM/WebSphere/AppServer/`

Input Parameters for Validate WebSphere 7 Deployment Manager Parameters, continued

Parameter Name	Example Value	Description
		profiles/ProdDmgr
Profile Type	management	Because this workflow creates a Deployment Manager profile, the value must be management.
Response File	/tmp/serverrsp	Fully qualified path where the response file that this workflow creates will be located. This file will then be used to drive the installation and profile creation.
Server Type	DEPLOYMENT_ MANAGER	The type of management profile. The value is DEPLOYMENT_ MANAGER for a deployment manager server.

Tip: To avoid having to re-enter passwords whenever they change, you can create a policy to provide them to the workflow.

Parameters for Provision WebSphere 7 and Deployment Manager

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

Note: Only those parameters that are configurable in a standard deployment are listed here. Input parameters that must be mapped to output parameters of previous steps are not listed.

Parameters Defined in this Step: Validate WebSphere 7 Deployment Manager Parameters

Parameter Name	Default Value	Required	Description
Admin Password	no default	optional	When Enable Security is set to true, this parameter must contain a string that does not begin with a dash(-) or contain a space( ).
Admin User	no default	optional	When Enable Security is set to true, this parameter must contain a string that does not begin with a dash(-), a period (.), or a space( ). It cannot contain any of the following characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }.
Binary Archive	no default	required	Fully qualified path to the compressed software package on the target machine. For example: `/opt/install/C1G36ML.tar.gz`
Call Wrapper	see description	required	Command that will execute this step (or subsequent steps) as a specific user. For UNIX targets, the default is: `/opt/hp/dma/client/jython.sh` running as root For Windows targets, the default is: `jython` running as Administrator This parameter is derived by the workflow. Under most circumstances, you should not change its mapping or its value.
Cell Name	no default	required	Unique cell name that does not contain any of the following special characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }. If you plan to federate into an existing cell later, make sure that this name is not the same as the existing cell name.
Default Ports	false	optional	Provides the option to assign default ports to a profile. Valid values are true or false. If true, the WebSphere Application Server default ports will be used, and the Ports File and Starting Port parameters should not have values. If false, the workflow will increment the default port until it finds a free port. The default value is false.

Parameters Defined in this Step: Validate WebSphere 7 Deployment Manager Parameters, continued

Parameter Name	Default Value	Required	Description
Enable Security	no default	required	Enables administrative security. Must be set to either true or false. If Enable Security is true, the Admin User and Admin Password parameters must have values.
Extract Dir	no default	required	Fully qualified path where the compressed software will be extracted on the target machine.
Host Name	Server.name	required	Hostname or IP address of the target machine.
Install Location	no default	required	Fully qualified path where WebSphere Application Server will be installed. For example: `/opt/IBM/WebSphere/AppServer`
Keystore Password	no default	required	Sets the password for all keystore files created during profile creation. This includes keystore files for both the default personal certificate and the root signing certificate.
License Acceptance	false	required	Acknowledges that the end user agrees to the IBM International Program License Agreement. This is set to false by default and must be set to true in order for the installation to continue.
Node Name	no default	required	Unique node name that cannot contain any of the following special characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }. If you plan to federate into an existing cell later, make sure that the name is unique within that cell.
Omit Action	no default	optional	Enables you to prevent certain optional features from being installed. Valid values are deployAdminConsole or defaultAppDeployAndConfig. You may only specify one of these options.
Personal CertDN	no default	optional	Distinguished name of the personal certificate. For example: CN=dmalab-example.com,OU=WAS7LabCell, OU=WAS7LabDmgrManager,O=IBM,C=US The DN string cannot contain spaces. If you do not specify the DN, the WebSphere Application Server installer will create one.
Personal CertValidity Period	1	optional	Amount of time in years that the personal certificate is valid. Default is one year.
Ports File	no default	optional	Fully qualified path to a file that defines port settings for the new profile. This file must contain key=value pairs that specify a service name and a port number (for example: WC_adminhost=9060). This option should be used with the Validate Ports option.

Parameters Defined in this Step: Validate WebSphere 7 Deployment Manager Parameters, continued

Parameter Name	Default Value	Required	Description
Profile Name	no default	required	A unique profile name. It cannot begin with a period (.) and cannot contain any of the following special characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }.
Profile Path	no default	required	Fully qualifed path to the Deployment Manager profile. For example: `/opt/IBM/WebSphere/AppServer/profiles/ProdDmgr`
Profile Type	management	required	Because this workflow creates a Deployment Manager profile, the value must be management.
Response File	no default	required	Fully qualified path where the response file that this workflow creates will be located. This file will then be used to drive the installation and profile creation.
Server Type	DEPLOYMENT_MANAGER	required	The type of management profile. The value is DEPLOYMENT_MANAGER for a deployment manager server.
Signing CertDN	no default	optional	Distinguished name of the signing certificate. For example: CN=dmalab-example.com, OU=Root Certificate, OU=WAS7TestLabCell, OU=WAS7LabNode1, O=IBM, C=US The DN string cannot contain spaces. If you do not specify the DN, the WebSphere Application Server installer will create one.
Signing CertValidity Period	15	optional	Amount of time in years that the root certificate is valid. Default is 15 years.
Starting Port	no default	optional	Starting port number that the profile will use to generate and assign port values. Port values are assigned sequentially from the Starting Port. Do not specify this parameter if you specify Default Ports or Ports File.
Validate Ports	no default	optional	Indicates that the ports should be validated to ensure that they are not already in use. Valid values are true or false. You should use this option if you specify a Ports File.
Windows Admin Password	no default	required	The Windows Administrator password. Required for Windows.
Windows Admin User	no default	required	This is the Windows Administrator user. Required for Windows.

Provision WebSphere 7 StandAlone Profile

Use this workflow to install the WebSphere 7 Base core binaries and, optionally, create a stand-alone profile.

A stand-alone application server works independently—it is not part of a cell and does not interact with a deployment manager. The stand-alone profile is not suitable for distributed application server environments.

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

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

Prerequisites for this Workflow

Be sure that the following prerequisites are satisfied before you run the Provision WebSphere 7 StandAlone Profile workflow:

1. This workflow requires unchallenged `sudo` access to a user (typically root) who can access all required files and directories.
2. Per the WebSphere 7 documentation, the following system libraries are required before provisioning IBM WebSphere Application Server version 7 on 64-bit Red Hat Linux:

Platform	Required Library
64-bit Red Hat Enterprise Linux version 5	compat-libstdc++-33-3.2.3-61 compat-db-4.2.52-5.1 libXp-1.0.0-8 compat-libstdc++- 296-2.96-138 rpm-build- 4.4.2-37.el5

   Make sure that these libraries exist on each target server before running this workflow. If newer versions of these libraries are available, you can install the newer versions.
3. This workflow will install WebSphere Application Server as root because of the following IBM documented limitations:
   - Creation of a Linux service for WebSphere Application Server
   - Native registration with the operating system
   - Port conflicts that may occur with other installations of WebSphere Application Server that are not registered with the operating system

   If there is a need to run as a non-root user after installation, you can run a recursive `chown` under the installation root and set owner permissions accordingly.

For more information about prerequisites for WebSphere 7, refer to the WebSphere 8 Product Documentation.

How this Workflow Works

This topic contains the following information about the Provision WebSphere 7 StandAlone Profile workflow:

Overview

This workflow does the following things in the order shown:

1. Prepares and validates all parameters and creates the call wrapper that will be used to execute commands within a WebSphere 7 environment
2. Checks the documented library requirements, files system space requirements, and temporary space requirements
3. Checks whether the WebSphere 7 binaries are available—if not, they will be downloaded from the software repository—and extracts the binary files from the compressed archive
4. Creates a new response file
5. Provisions IBM WebSphere Application Server version 7 on a target machine
6. Creates a stand-alone profile
7. Starts the stand-alone WebSphere Application Server V7.0

Validation Checks Performed

Most of the validation centers on special characters and spaces in the parameters. There are also validation checks that happen at the operating system level, including file system space checks and RPM checks for Red Hat Linux.

The workflow first performs the following parameter checks:

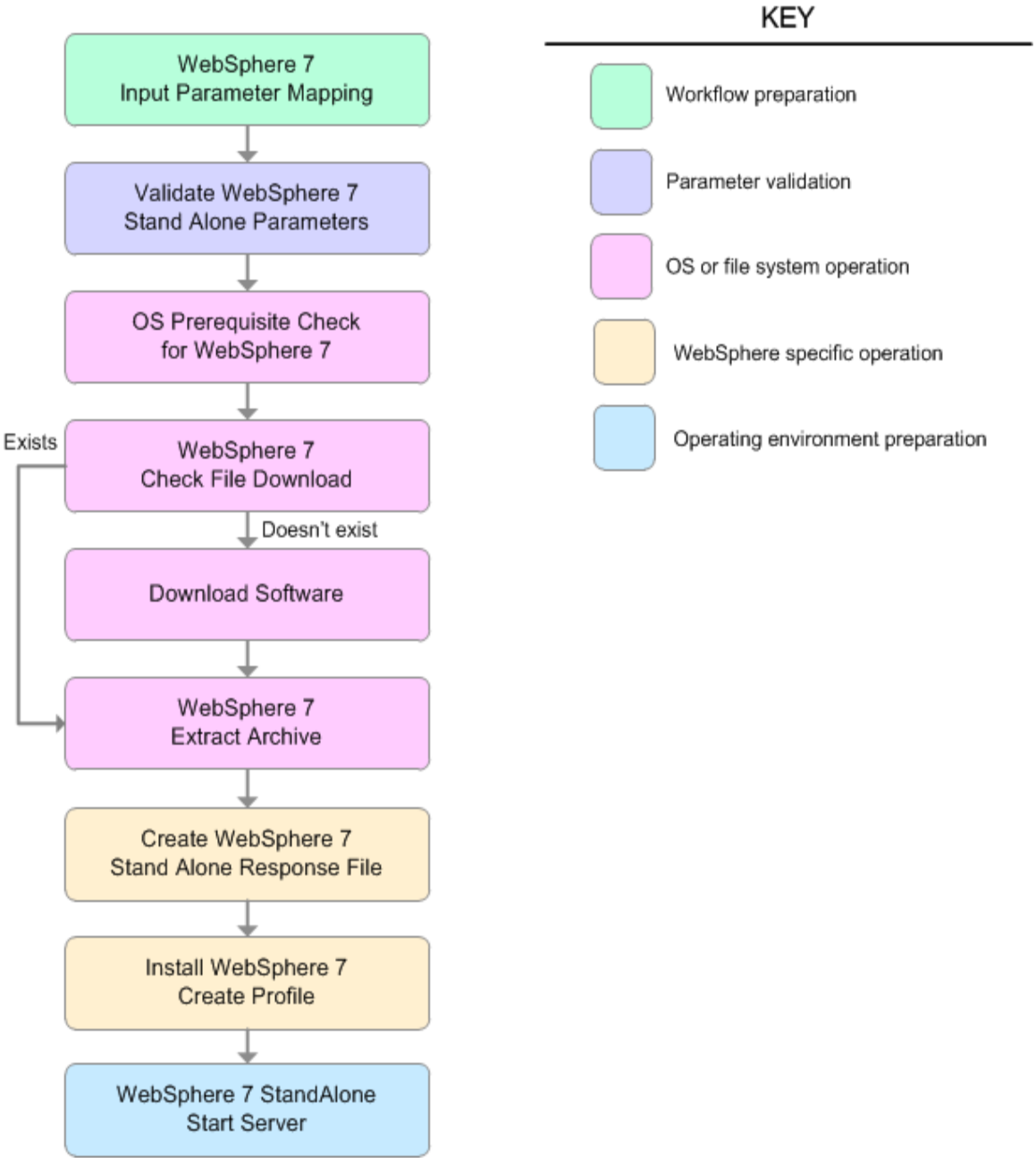
1. Binary Archive is specified. It either exists or can be created successfully.
2. Extract Path and Install Location either exist or can be created successfully.
3. Admin User (if specified) does not begin with a period (.), hyphen (-) or space. It does not contain any of the following characters: / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }
4. Admin Password (if specified) does not begin with a hyphen (-) or contain a space.
5. Cell Name, Node Name, Profile Name, and Server Name are specified. They do not contain the following characters: / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { } or space. They do not begin with a period.
6. Host Name is specified.
7. Default Ports and Developer Server (if specified) are true or false.
8. Enable Security is true or false. If Enable Security is true, Admin Password and Admin User are specified.
9. License Acceptance is true.
10. Omit Action (if specified) is defaultAppDeployAndConfig, or deployAdminConsole.
11. Ports File (if specified) exists and Validate Ports is true or false.
12. Starting Port (if specified) is an integer.
13. If the operating system is Windows, Windows Admin User and Windows Admin Password are specified.
14. Profile Path and Response File are specified.
15. Profile Type is standAlone.

The workflow then performs the following operating system checks on the target machine:

1. All required libraries are present (see "Prerequisites for this Workflow" on page 144).
2. Sufficient disk space is available to install WebSphere 7.
3. Sufficient disk space is available to extract the binary files from the compressed archive.

Steps Executed

The Provision WebSphere 7 StandAlone Profile workflow includes the following steps. Each step must complete successfully before the next step can start. If a step fails, the workflow reports a failure, and all subsequent steps are skipped.



Steps Used in the Provision WebSphere 7 StandAlone Profile Workflow

Workflow Step	Description
WebSphere 7 Input Parameter Mapping	This step creates the call wrapper—the command that executes the step as a specific user—and allows certain parameters to be hidden or exposed.
Validate WebSphere 7 Stand Alone Parameters	This step prepares and validates the parameters needed to install WebSphere Application Server V7.0 and create a stand-alone profile.
OS Prerequisite Check for WebSphere 7	This step checks the documented library requirements, files system space requirements, and temporary space requirements for WebSphere Application Server V7.0.
WebSphere 7 Check File Download	This step checks for the existence of a file before downloading it from the software repository: • Checks if a file exists in the expected location. • If the file is not in the expected location, the file is added to a list of files that need to be downloaded.
Download Software	This step downloads a list of files to a specified location on the target server.
WebSphere 7 Extract Archive	This step checks that the archive file exists and then, based on the archive extension, extracts the archive to the specified directory.
Create WebSphere 7 Stand Alone Response File	This step creates a new response file for installing a new instance of WebSphere Application Server V7.0 and creating a stand-alone profile.
Install WebSphere 7 Create Profile	This step installs a new instance of WebSphere Application Server V7.0 using the `install -options <responsefile> silent` option and then creates a profile.
WebSphere 7 StandAlone Start Server	This step starts the stand-alone WebSphere Application Server V7.0.

For parameter descriptions and defaults, see "Parameters for Provision WebSphere 7 StandAlone Profile" on page 154.

How to Run this Workflow

The following instructions show you how to customize and run the Provision WebSphere 7 StandAlone Profile in your environment.

The workflow provides default values for some parameters. These default values are usually sufficient for a "typical" installation. You can override the defaults by specifying parameter values in the deployment. You can also expose additional parameters in the workflow, if necessary, to accomplish more advanced scenarios. Any parameters not explicitly specified in the deployment will have the default values listed in "Parameters for Provision WebSphere 7 StandAlone Profile" on page 154.

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

To customize and run the Provision WebSphere 7 StandAlone Profile workflow:

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

Input Parameters for Validate WebSphere 7 Stand Alone Parameters

Parameter Name	Default Value	Required	Description
Admin Password	no default	optional	When Enable Security is set to true, this parameter must contain a string that does not begin with a dash(-) or contain a space( ).
Admin User	no default	optional	When Enable Security is set to true, this parameter must contain a string that does not begin with a dash(-), a period(.), or a space( ). It cannot contain any of the following characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }.
Binary Archive	no default	required	Fully qualified path to the compressed software package on the target machine. For example: `/opt/install/C1G36ML.tar.gz`
Cell Name	no default	required	Unique cell name that does not contain any of the following special characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }. If you plan to federate into an existing cell later, make sure that this name is not the same as the existing cell name.
Enable Security	no default	required	Enables administrative security. Must be set to either true or false. If Enable Security is true, the Admin User and Admin Password parameters must have values.
Extract Dir	no default	required	Fully qualified path where the compressed software will be extracted on the target machine.
Install Location	no default	required	Fully qualified path where WebSphere Application Server will be installed. For example:

Input Parameters for Validate WebSphere 7 Stand Alone Parameters, continued

Parameter Name	Default Value	Required	Description
			`/opt/IBM/WebSphere/AppServer`
License Acceptance	false	required	Acknowledges that the end user agrees to the IBM International Program License Agreement. This is set to false by default and must be set to true in order for the installation to continue.
Node Name	no default	required	Unique node name that cannot contain any of the following special characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }. If you plan to federate into an existing cell later, make sure that the name is unique within that cell.
Profile Name	no default	required	A unique profile name. It cannot begin with a period (.) and cannot contain any of the following special characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }.
Profile Path	no default	required	Fully qualifed path to the stand-alone profile. For example: `/opt/IBM/WebSphere/AppServer/profiles/AppServer1`
Profile Type	standAlone	required	Because this workflow creates a stand-alone profile, the value is standAlone.
Response File	no default	required	Fully qualified path where the response file that this workflow creates will be located. This file will then be used to drive the installation and profile creation.
Server Name	no default	required	Name of the application server that will be created under the profile.
Windows Admin Password	no default	required	The Windows Administrator password. Required for Windows.
Windows Admin User	no default	required	This is the Windows Administrator user. Required for Windows.

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

See "Parameters for Provision WebSphere 7 StandAlone Profile" on page 154 for detailed descriptions of all input parameters for this workflow, including default values.

Tip: To avoid having to re-enter passwords whenever they change, you can create a policy to provide them to the workflow.

3. n the workflow editor, expose any additional parameters that you need. You will specify values for those

parameters when you create the deployment.

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

To verify the results:

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

Optional: if you want to further verify the results, perform the following steps:

1. After the workflow has completed, run the following command to check the version of WebSphere Application Server that was installed:

   WAS_ROOT/bin/versionInfo.sh

   Here, *WAS_ROOT* is the directory where WebSphere 7 is installed. This is the path that you specified in the WebSphere Install Location parameter.
2. Validate that stand-alone profile has been created and is running by doing the following:
   a. View the *WAS_ROOT*/profiles/*PROFILE_NAME*/logs/AboutThisProfile.txt file. This file is created after the creation of the profile and contains specific information about the profile.

      Here, *PROFILE_NAME* is the name of the profile that you just created. This is the name that you specified in the Profile Name parameter.

   b. Change to the *WAS_ROOT*/profiles/*PROFILE_NAME*/logs/*SERVER_NAME* directory, and tail the SystemOut.log file. Look for the following line:

      Server *SERVER_NAME* open for e-business

      Here, *SERVER_NAME* is the name of the application server that you just created. This is the name that you specified in the Server Name parameter.

Sample Scenario

This topic shows you typical parameter values used for the Provision WebSphere 7 StandAlone Profile workflow.

New WebSphere 7 install with stand-alone profile

Input Parameters for Validate WebSphere 7 Stand Alone Parameters

Parameter Name	Example Value	Description
Admin Password	wasPassWord	When Enable Security is set to true, this parameter must contain a string that does not begin with a dash(-) or contain a space( ).
Admin User	wasadmin	When Enable Security is set to true, this parameter must contain a string that does not begin with a dash(-), a period(.), or a space( ). It cannot contain any of the following characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }.
Binary Archive	see description	Fully qualified path to the compressed software package on the target machine. For example: `/opt/install/C1G36ML.tar.gz`
Cell Name	DevCell	Unique cell name that does not contain any of the following special characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }. If you plan to federate into an existing cell later, make sure that this name is not the same as the existing cell name.
Enable Security	true	Enables administrative security. Must be set to either true or false. If Enable Security is true, the Admin User and Admin Password parameters must have values.
Extract Dir	`/opt/IBM/wasv7`	Fully qualified path where the compressed software will be extracted on the target machine.
Install Location	see description	Fully qualified path where WebSphere Application Server will be installed. For example: `/opt/IBM/WebSphere/AppServer`
License Acceptance	true	Acknowledges that the end user agrees to the IBM International Program License Agreement. This is set to false by default and must be set to true in order for the installation to continue.
Node Name	DevStandAlone1Node	Unique node name that cannot contain any of the following special characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }. If you plan to federate into an existing cell later, make sure that the name is unique within that cell.
Profile Name	StandAlone1	A unique profile name. It cannot begin with a period (.) and cannot contain any of the following special characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }.
Profile Path	see description	Fully qualifed path to the stand-alone profile. For example: `/opt/IBM/WebSphere/AppServer/`

Input Parameters for Validate WebSphere 7 Stand Alone Parameters, continued

Parameter Name	Example Value	Description
		profiles/AppServer1
Profile Type	standAlone	Because this workflow creates a stand-alone profile, the value is standAlone.
Response File	/tmp/serverrsp	Fully qualified path where the response file that this workflow creates will be located. This file will then be used to drive the installation and profile creation.
Server Name	Server1	Name of the application server that will be created under the profile.

Parameters for Provision WebSphere 7 StandAlone Profile

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

Parameters Defined in this Step: Validate WebSphere 7 Stand Alone Parameters

Parameter Name	Default Value	Required	Description
Admin Password	no default	optional	When Enable Security is set to true, this parameter must contain a string that does not begin with a dash(-) or contain a space( ).
Admin User	no default	optional	When Enable Security is set to true, this parameter must contain a string that does not begin with a dash(-), a period(.), or a space( ). It cannot contain any of the following characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }.
Binary Archive	no default	required	Fully qualified path to the compressed software package on the target machine. For example: `/opt/install/C1G36ML.tar.gz`
Call Wrapper	see description	required	Command that will execute this step (or subsequent steps) as a specific user. For UNIX targets, the default is: `/opt/hp/dma/client/jython.sh` running as root For Windows targets, the default is: `jython` running as Administrator This parameter is derived by the workflow. Under most circumstances, you should not change its mapping or its value.
Cell Name	no default	required	Unique cell name that does not contain any of the following special characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }. If you plan to federate into an existing cell later, make sure that this name is not the same as the existing cell name.
Default Ports	false	optional	Provides the option to assign default ports to a profile. Valid values are true or false. If true, the WebSphere Application Server default ports will be used, and the Ports File and Starting Port parameters should not have values. If false, the workflow will increment the default port until it finds a free port. The default value is false.
Developer Server	no default	optional	Use this parameter for development environments only to help with start up time. Valid value is true. Do not use in production environments.

Parameters Defined in this Step: Validate WebSphere 7 Stand Alone Parameters, continued

Parameter Name	Default Value	Required	Description
Enable Security	no default	required	Enables administrative security. Must be set to either true or false. If Enable Security is true, the Admin User and Admin Password parameters must have values.
Extract Dir	no default	required	Fully qualified path where the compressed software will be extracted on the target machine.
Host Name	Server.name	required	Hostname or IP address of the target machine.
Install Location	no default	required	Fully qualified path where WebSphere Application Server will be installed. For example: `/opt/IBM/WebSphere/AppServer`
Keystore Password	no default	optional	Sets the password for all keystore files created during profile creation. This includes keystore files for both the default personal certificate and the root signing certificate.
License Acceptance	false	required	Acknowledges that the end user agrees to the IBM International Program License Agreement. This is set to false by default and must be set to true in order for the installation to continue.
Node Name	no default	required	Unique node name that cannot contain any of the following special characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }. If you plan to federate into an existing cell later, make sure that the name is unique within that cell.
Omit Action	no default	optional	Enables you to prevent certain optional features from being installed. Valid values are deployAdminConsole or defaultAppDeployAndConfig. You may only specify one of these options.
Personal CertDN	no default	optional	Distinguished name of the personal certificate. For example: CN=dmalab-example.com,OU=WAS7LabCell, OU=WAS7LabDmgrManager,O=IBM,C=US The DN string cannot contain spaces. If you do not specify the DN, the WebSphere Application Server installer will create one.
Personal CertValidity Period	1	optional	Amount of time in years that the personal certificate is valid. Default is one year.
Ports File	no default	optional	Fully qualified path to a file that defines port settings for the new profile. This file must contain key=value pairs that specify a service name and a port number (for example: WC_ adminhost=9060). This option should be used with the Validate Ports option.
Profile Name	no default	required	A unique profile name. It cannot begin with a period (.) and cannot contain any of the following special characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }.

Parameters Defined in this Step: Validate WebSphere 7 Stand Alone Parameters, continued

Parameter Name	Default Value	Required	Description
Profile Path	no default	required	Fully qualifed path to the stand-alone profile. For example: `/opt/IBM/WebSphere/AppServer/profiles/AppServer1`
Profile Type	standAlone	required	Because this workflow creates a stand-alone profile, the value is standAlone.
Response File	no default	required	Fully qualified path where the response file that this workflow creates will be located. This file will then be used to drive the installation and profile creation.
Server Name	no default	required	Name of the application server that will be created under the profile.
Signing CertDN	no default	optional	Distinguished name of the signing certificate. For example: CN=dmalab-example.com, OU=Root Certificate, OU=WAS7TestLabCell, OU=WAS7LabNode1, O=IBM, C=US The DN string cannot contain spaces. If you do not specify the DN, the WebSphere Application Server installer will create one.
Signing CertValidity Period	15	optional	Amount of time in years that the root certificate is valid. Default is 15 years.
Starting Port	no default	optional	Starting port number that the profile will use to generate and assign port values. Port values are assigned sequentially from the Starting Port. Do not specify this parameter if you specify Default Ports or Ports File.
Validate Ports	no default	optional	Indicates that the ports should be validated to ensure that they are not already in use. Valid values are true or false. You should use this option if you specify a Ports File.
Windows Admin Password	no default	required	The Windows Administrator password. Required for Windows.
Windows Admin User	no default	required	This is the Windows Administrator user. Required for Windows.

Provision IBM HTTP Server 7 and Plug-In

Use this workflow to install IBM HTTP Server for WebSphere Application Server V7.0 and, optionally, install its WebSphere Application Server Plug-In.

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

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

Prerequisites for this Workflow

Be sure that the following prerequisites are satisfied before you run the Provision IBM HTTP Server 7 and Plug-In workflow:

1. This workflow requires unchallenged `sudo` access to a user (typically root) who can access all required files and directories.
2. Per the WebSphere 7 documentation, the following system libraries are required before provisioning IBM WebSphere Application Server version 7 on 64-bit Red Hat Linux:

Platform	Required Library
64-bit Red Hat Enterprise Linux version 5	compat-libstdc++-33-3.2.3-61 compat-db-4.2.52-5.1 libXp-1.0.0-8 compat-libstdc++- 296-2.96-138 rpm-build- 4.4.2-37.el5

   Make sure that these libraries exist on each target server before running this workflow. If newer versions of these libraries are available, you can install the newer versions.
3. This workflow will install WebSphere Application Server as root because of the following IBM documented limitations:
   - Creation of a Linux service for WebSphere Application Server
   - Native registration with the operating system
   - Port conflicts that may occur with other installations of WebSphere Application Server that are not registered with the operating system

   If there is a need to run as a non-root user after installation, you can run a recursive `chown` under the installation root and set owner permissions accordingly.

For more information about prerequisites for WebSphere 7, refer to the WebSphere 7 Product Documentation.

How this Workflow Works

This topic contains the following information about the Provision IBM HTTP Server 7 and Plug-In workflow:

Overview

This workflow does the following things in the order shown:

1. Prepares and validates all parameters and creates the call wrapper that will be used to execute commands within a WebSphere 7 environment
2. Checks the documented library requirements, files system space requirements, and temporary space requirements
3. Checks whether the WebSphere 7 binaries are available—if not, they will be downloaded from the software repository—and extracts the binary files from the compressed archive
4. Creates a new response file for installing IBM HTTP Server and creating its plug-in
5. Installs IBM HTTP Server

Validation Checks Performed

Most of the validation centers on special characters and spaces in the parameters. There are also validation checks that happen at the operating system level, including file system space checks and RPM checks for Red Hat Linux.

The workflow first performs the following parameter checks:

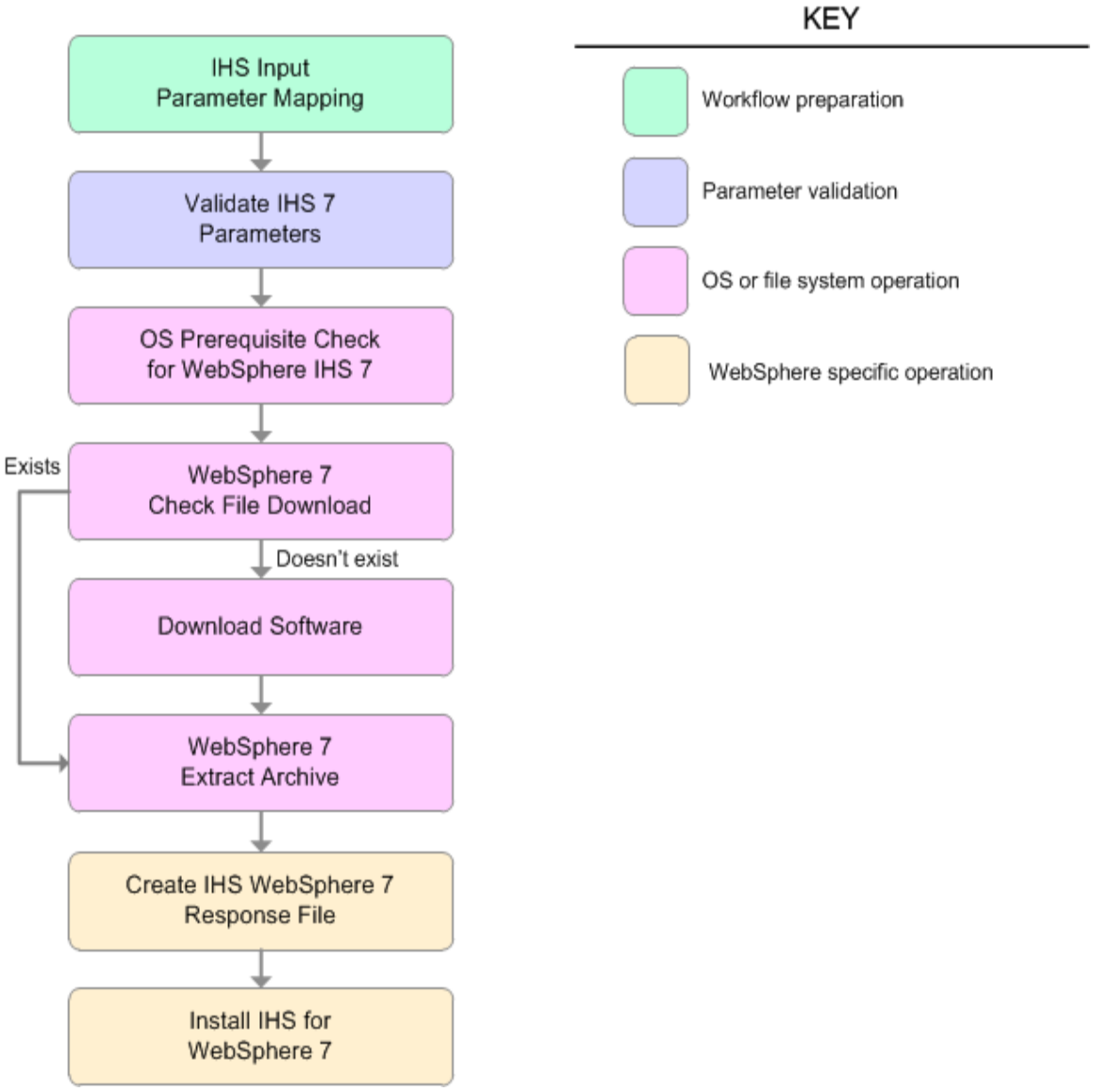
1. If Create Admin Auth is true, Admin Auth User, Admin Auth Password, and Admin Auth Password Confirm are specified.
2. If Create Admin User Group is true, Set Up Admin User and Set Up Admin Group are specified.
3. If Install Plugin is true, WebSphere Hostname is specified.
4. Binary Archive is a full file path.The directory path either exists or can be created successfully.
5. Extract Dir and Install Location are full directory paths. The directory paths either exist or can be created successfully.
6. Admin Auth User does not contain a colon (:).
7. Webserver Definition and WebSphere Hostname do not contain a space ( ).
8. Http Port and Admin Port (if specified) are integers.
9. License Acceptance, Create Admin Auth, Run Admin Setup, Create Admin User Group, and Install Plugin are true or false (case insensitive).

The workflow then performs the following operating system checks on the target machine:

1. All required libraries are present (see "Prerequisites for this Workflow" on the previous page).
2. Sufficient disk space is available to install IBM HTTP Server for WebSphere Application Server V7.0.
3. Sufficient disk space is available to extract the binary files from the compressed archive.

Steps Executed

The Provision IBM HTTP Server 7 and Plug-In workflow includes the following steps. Each step must complete successfully before the next step can start. If a step fails, the workflow reports a failure, and all subsequent steps are skipped.



Steps Used in the Provision IBM HTTP Server 7 and Plug-In Workflow

Workflow Step	Description
IHS Input Parameter Mapping	This step allows for either the defaulting of parameters to be used later in a step or to hide or expose certain parameters that will or will not be needed depending on what the end user wants to do.
Validate IHS 7 Parameters	This step prepares and validates the parameters needed to install IBM HTTP Server for WebSphere Application Server V7.0 and, optionally, create its WebSphere Application Server plug-in.
OS Prerequisite Check for WebSphere IHS 7	This step checks the following: 1. Documented library requirements for WebSphere Application Server V7.0. 2. Files system space requirements where IBM HTTP Server for WebSphere Application Server V7.0 will be installed.. 3. Temporary space requirements where the compressed software will be extracted before it is installed.
WebSphere 7 Check File Download	This step checks for the existence of a file before downloading it from the software repository: • Checks if a file exists in the expected location. • If the file is not in the expected location, the file is added to a list of files that need to be downloaded.
Download Software	This step downloads a list of files to a specified location on the target server.
WebSphere 7 Extract Archive	This step checks that the archive file exists and then, based on the archive extension, extracts the archive to the specified directory.
Create IHS WebSphere 7 Response File	This step creates a new response file for installing IBM HTTP Server for WebSphere Application Server V7.0 and then, optionally, creating its WebSphere Application Server plug-in.
Install IHS for WebSphere 7	This step installs IBM HTTP Server for WebSphere Application Server V7.0 using the "install -options <responsefile> silent" option.

How to Run this Workflow

The following instructions show you how to customize and run the Provision IBM HTTP Server 7 and Plug-In workflow in your environment.

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

To customize and run the Provision IBM HTTP Server 7 and Plug-Inworkflow:

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

Input Parameters for Validate IHS 7 Parameters

Parameter Name	Default Value	Required	Description
Admin Auth Password	no default	optional	The password used to authenticate to the IBM HTTP administration server using the WebSphere Application Server administrative console. When Create Admin Auth is set to true, this parameter must have a value. It cannot begin with a dash(-) or contain a space( ).
Admin Auth Password Confirm	no default	optional	Confirms the Admin Auth Password.
Admin Auth User	no default	optional	The user ID used to authenticate to the IBM HTTP administration server using the WebSphere Application Server administrative console. When Create Admin Auth is set to true, this parameter must have a value. It cannot begin with a dash(-), a period(.), or a space( ) and cannot contain any of the following characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }
Admin Port	no default	required	The port on which the HTTP administration web server will run. This is usually 8008.
Binary Archive	no default	required	Fully qualified path to the compressed software package on the target machine. For example: `/opt/install/C1G36ML.tar.gz`
Create Admin Auth	no default	required	Set this to true to create a user ID and password to authenticate to the IBM HTTP administration server using the WebSphere Application Server administrative console. If this parameter is set to true, the following parameters must have values: Admin Auth Password, Admin Auth Password Confirm, and Admin Auth User.
Create Admin User	no default	required	Set to true to create a user ID and group used to set up the IBM HTTP Administration Server on Linux and UNIX operating

Input Parameters for Validate IHS 7 Parameters, continued

Parameter Name	Default Value	Required	Description
Group			systems.
Extract Dir	no default	required	Fully qualified path where the compressed software will be extracted on the target machine.
Http Port	no default	required	The port on which the web server will listen. This is usually set to 80.
Install Location	no default	required	Fully qualified path where IBM HTTP Server will be installed. For example: `/opt/IBM/HTTPServer`
Install Plugin	no default	required	Determines whether or not the WebSphere Application Server Plug-In is installed. Valid options are true or false.
License Acceptance	false	required	Acknowledges that the end user agrees to the IBM International Program License Agreement. This is set to false by default and must be set to true in order for the installation to continue.
Response File	no default	required	Fully qualified path where the response file that this workflow creates will be located. This file is used to drive the installation.
Run Admin Setup	no default	required	Enables the install process to grant the Set Up Admin User write access to the necessary IBM HTTP Server and WebSphere Application Server Plug-In configuration files. Valid options are true or false.
Set Up Admin Group	no default	optional	Group name used to set up the IBM HTTP administration server on Linux and UNIX operating systems. This parameter must have a value if Create Admin User Group is set to true.
Set Up Admin User	no default	optional	User ID used to set up the IBM HTTP administration server on Linux and UNIX operating systems. If Create Admin User Group is set to true, this parameter must have a value.
Webserver Definition	no default	optional	A web server definition allows for web server administration through the WebSphere administrative console. This parameter must be set if the Install Plugin parameter is set to true. An example would be webserver1. No spaces are allowed in the Webserver Definition name.
WebSphere Hostname	no default	optional	Host name of the WebSphere Application Server machine. This parameter is required if Install Plugin is set to true. No spaces are allowed in the host name.

Additional Input Parameters for Install IHS for WebSphere 7

Parameter Name	Default Value	Required	Description
Password	no default	required	The Windows Administrator password. Required for Windows.
Username	no default	required	This is the Windows Administrator user. Required for Windows.

Note: See "Parameters for Provision IBM HTTP Server 7 and Plug-in" for detailed descriptions of all input parameters for this workflow, including default values.

Tip: To avoid having to re-enter passwords whenever they change, you can create a policy to provide them to the workflow.

3. Save the changes to the workflow (click **Save** in the lower right corner).
4. Create a new deployment.
5. On the Parameters tab, specify values for the required parameters listed in step 2.
6. On the Targets tab, specify one or more targets for this deployment.
7. Save the deployment (click **Save** in the lower right corner).
8. Run the workflow using this deployment.

To verify the results:

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

Optional: if you want to further verify the results, perform the following steps:

1. After the workflow has completed, run the following command to check the version IBM HTTP Server that was installed:

   IHS_ROOT/bin/versionInfo.sh

   Here, *IHS_ROOT* is the directory where IBM HTTP Server is installed. This is the path that you specified in the WebSphere Install Location parameter.
2. Validate that the IBM HTTP Server has been properly installed by doing the following:

   View the *IHS_ROOT*/logs/install/log.txt file.

   If the installation was successful, you should see messages similar to these:

   ```
   (Apr 21, 2011 9:21:06 AM), Process,
   com.ibm.ws.install.ni.ismp.actions.SettleNIFRegistryAction, msg1, Current
   install/uninstall process is successful. Process type is: install
   ```

   ```
   (Apr 21, 2011 9:21:07 AM), Process,
   com.ibm.ws.install.ni.ismp.actions.SetExitCodeAction, msg1, CWUPI0000I: EXITCODE=0
   ```

   ```
   (Apr 21, 2011 9:21:07 AM), Process,
   com.ibm.ws.install.ni.ismp.actions.ISMPLogSuccessMessageAction, msg1,
   INSTCONFSUCCESS
   ```
3. If you installed the WebSphere Application Server Plug-In, validate that it has been properly installed by doing the following:

   View the *IHS_ROOT*/Plugins/logs/install/log.txt file.

   If the installation was successful, you should see messages similar to these:

   ```
   (Apr 21, 2011 9:21:05 AM), Process,
   com.ibm.ws.install.ni.ismp.actions.ISMPLogFileAction, msg1, INSTCONF_COMPLETE :
   Installation is complete.
   ```

   ```
   (Apr 21, 2011 9:21:05 AM), Process,
   com.ibm.ws.install.ni.ismp.actions.ISMPLogFileAction, msg1,
   ***************************
   ```

   ```
   (Apr 21, 2011 9:21:05 AM), Process,
   com.ibm.ws.install.ni.ismp.actions.SetExitCodeAction, msg1, CWUPI0000I: EXITCODE=0
   ```

   ```
   (Apr 21, 2011 9:21:05 AM), Process,
   com.ibm.ws.install.ni.ismp.actions.ISMPLogSuccessMessageAction, msg1,
   INSTCONFSUCCESS
   ```

Sample Scenario

This topic shows you typical parameter values used for the Provision IBM HTTP Server 7 and Plug-In workflow.

Scenario 1: New IBM HTTP Server install with plug-in using the simplest method

This example shows the following:

Task	Parameter Values
Do not create a user ID and password to authenticate to the IBM HTTP administration server using the WebSphere Application Server administrative console	• Set Create Admin Auth to false
Do not create a user ID and group used to set up the IBM HTTP Administration Server on Linux and UNIX operating systems	• Set Create Admin User Group to false
Do not install the WebSphere Application Server Plug-In	• Set Install Plugin to false
Do not grant the Set Up Admin User write access to the necessary IBM HTTP Server and WebSphere Application Server Plug-In configuration files	• Set Run Admin Setup to false

Input Parameters for Validate IHS 7 Parameters

Parameter Name	Example Value	Description
Admin Port	8008	The port on which the HTTP administration web server will run. This is usually 8008.
Binary Archive	see description	Fully qualified path to the compressed software package on the target machine. For example: `/opt/install/C1G36ML.tar.gz`
Create Admin Auth	false	Set this to true to create a user ID and password to authenticate to the IBM HTTP administration server using the WebSphere Application Server administrative console. If this parameter is set to true, the following parameters must have values: Admin Auth Password, Admin Auth Password Confirm, and Admin Auth User.
Create Admin User Group	false	Set to true to create a user ID and group used to set up the IBM HTTP Administration Server on Linux and UNIX operating systems.
Extract Dir	`/opt/IBM/wasv7`	Fully qualified path where the compressed software will be extracted on the target machine.
Http Port	80	The port on which the web server will listen. This is usually set to 80.
Install Location	see description	Fully qualified path where IBM HTTP Server will be installed. For example: `/opt/IBM/HTTPServer`

Input Parameters for Validate IHS 7 Parameters, continued

Parameter Name	Example Value	Description
Install Plugin	false	Determines whether or not the WebSphere Application Server Plug-In is installed. Valid options are true or false.
License Acceptance	true	Acknowledges that the end user agrees to the IBM International Program License Agreement. This is set to false by default and must be set to true in order for the installation to continue.
Response File	`/tmp/serverrsp`	Fully qualified path where the response file that this workflow creates will be located. This file is used to drive the installation.
Run Admin Setup	false	Enables the install process to grant the Set Up Admin User write access to the necessary IBM HTTP Server and WebSphere Application Server Plug-In configuration files. Valid options are true or false.

Scenario 2: New IBM HTTP Server install with plug-in using all the options

This example shows the following:

Task	Parameter Values
To create a user ID and password to authenticate to the IBM HTTP administration server using the WebSphere Application Server administrative console	• Set Create Admin Auth to true • Specify values for: Admin Auth Password Admin Auth Password Confirm Admin Auth User
To create a user ID and group used to set up the IBM HTTP Administration Server on Linux and UNIX operating systems	• Set Create Admin User Group to true • Specify values for: Set Up Admin Group Set Up Admin User
To install the WebSphere Application Server Plug-In	• Set Install Plugin to true • Specify values for: WebSphere Hostname Webserver Definition
To grant the Set Up Admin User write access to the necessary IBM HTTP Server and WebSphere Application Server Plug-In configuration files	• Set Run Admin Setup to true

Input Parameters for Validate IHS 7 Parameters

Parameter Name	Example Value	Description
Admin Auth Password	AdminPsWd	The password used to authenticate to the IBM HTTP administration server using the WebSphere Application Server administrative console. When Create Admin Auth is set to true, this parameter must have a value. It cannot begin with a dash(-) or contain a space( ).
Admin Auth Password Confirm	AdminPsWd	Confirms the Admin Auth Password.
Admin Auth User	admin	The user ID used to authenticate to the IBM HTTP administration server using the WebSphere Application Server administrative console. When Create Admin Auth is set to true, this parameter must have a value. It cannot begin with a dash(-), a period(.), or a space( ) and cannot contain any of the following characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }
Admin Port	8008	The port on which the HTTP administration web server will run. This is usually 8008.
Binary Archive	see description	Fully qualified path to the compressed software package on the target machine.

Input Parameters for Validate IHS 7 Parameters, continued

Parameter Name	Example Value	Description
		For example: `/opt/install/C1G36ML.tar.gz`
Create Admin User Group	false	Set to true to create a user ID and group used to set up the IBM HTTP Administration Server on Linux and UNIX operating systems.
Extract Dir	`/opt/IBM/wasv7`	Fully qualified path where the compressed software will be extracted on the target machine.
Http Port	80	The port on which the web server will listen. This is usually set to 80.
Install Location	see description	Fully qualified path where IBM HTTP Server will be installed. For example: `/opt/IBM/HTTPServer`
Install Plugin	false	Determines whether or not the WebSphere Application Server Plug-In is installed. Valid options are true or false.
License Acceptance	true	Acknowledges that the end user agrees to the IBM International Program License Agreement. This is set to false by default and must be set to true in order for the installation to continue.
Response File	`/tmp/serverrsp`	Fully qualified path where the response file that this workflow creates will be located. This file is used to drive the installation.
Run Admin Setup	false	Enables the install process to grant the Set Up Admin User write access to the necessary IBM HTTP Server and WebSphere Application Server Plug-In configuration files. Valid options are true or false.
Set Up Admin Group	AdminGrp	Group name used to set up the IBM HTTP administration server on Linux and UNIX operating systems. This parameter must have a value if Create Admin User Group is set to true.
Set Up Admin User	AdminUsr	User ID used to set up the IBM HTTP administration server on Linux and UNIX operating systems. If Create Admin User Group is set to true, this parameter must have a value.
Webserver Definition	webserver1	A web server definition allows for web server administration through the WebSphere administrative console. This parameter must be set if the Install Plugin parameter is set to true. An example would be webserver1. No spaces are allowed in the Webserver Definition name.
WebSphere Hostname	was1.mycompany.com	Host name of the WebSphere Application Server machine. This parameter is required if Install Plugin is set to true. No spaces are allowed in the host name.
Admin Auth Password	AdminPsWd	The password used to authenticate to the IBM HTTP administration server using the WebSphere Application Server

Input Parameters for Validate IHS 7 Parameters, continued

Parameter Name	Example Value	Description
		administrative console. When Create Admin Auth is set to true, this parameter must have a value. It cannot begin with a dash(-) or contain a space( ).

Parameters for Provision IBM HTTP Server 7 and Plug-in

The following tables describe the required and optional input parameters for this workflow. For most parameters, if you do not specify a value for a parameter, a default value is assigned.

Note: Only those parameters that are configurable in a standard deployment are listed here. Input parameters that must be mapped to output parameters of previous steps are not listed.

Parameters Defined in this Step: Validate IHS 7 Parameters

Parameter Name	Default Value	Required	Description
Admin Auth Password	default	optional	The password used to authenticate to the IBM HTTP administration server using the WebSphere Application Server administrative console. When Create Admin Auth is set to true, this parameter must have a value. It cannot begin with a dash(-) or contain a space( ).
Admin Auth Password Confirm	default	optional	Confirms the Admin Auth Password.
Admin Auth User	default	optional	The user ID used to authenticate to the IBM HTTP administration server using the WebSphere Application Server administrative console. When Create Admin Auth is set to true, this parameter must have a value. It cannot begin with a dash(-), a period(.), or a space( ) and cannot contain any of the following characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }
Admin Port	default	required	The port on which the HTTP administration web server will run. This is usually 8008.
Binary Archive	default	required	Fully qualified path to the compressed software package on the target machine. For example: `/opt/install/C1G36ML.tar.gz`
Call Wrapper	see description	required	Command that will execute this step (or subsequent steps) as a specific user. For UNIX targets, the default is: `/opt/hp/dma/client/jython.sh` running as root For Windows targets, the default is: `jython` running as Administrator This parameter is derived by the workflow. Under most circumstances, you should not change its mapping or its value.
Create Admin Auth	default	required	Set this to true to create a user ID and password to authenticate to the IBM HTTP administration server using the WebSphere Application Server administrative console. If this parameter is set

Parameters Defined in this Step: Validate IHS 7 Parameters, continued

Parameter Name	Default Value	Required	Description
			to true, the following parameters must have values: Admin Auth Password, Admin Auth Password Confirm, and Admin Auth User.
Create Admin User Group	default	required	Set to true to create a user ID and group used to set up the IBM HTTP Administration Server on Linux and UNIX operating systems.
Extract Dir	default	required	Fully qualified path where the compressed software will be extracted on the target machine.
Http Port	default	required	The port on which the web server will listen. This is usually set to 80.
Install Location	default	required	Fully qualified path where IBM HTTP Server will be installed. For example: `/opt/IBM/HTTPServer`
Install Plugin	default	required	Determines whether or not the WebSphere Application Server Plug-In is installed. Valid options are true or false.
License Acceptance	false	required	Acknowledges that the end user agrees to the IBM International Program License Agreement. This is set to false by default and must be set to true in order for the installation to continue.
Response File	default	required	Fully qualified path where the response file that this workflow creates will be located. This file is used to drive the installation.
Run Admin Setup	default	required	Enables the install process to grant the Set Up Admin User write access to the necessary IBM HTTP Server and WebSphere Application Server Plug-In configuration files. Valid options are true or false.
Set Up Admin Group	default	optional	Group name used to set up the IBM HTTP administration server on Linux and UNIX operating systems. This parameter must have a value if Create Admin User Group is set to true.
Set Up Admin User	default	optional	User ID used to set up the IBM HTTP administration server on Linux and UNIX operating systems. If Create Admin User Group is set to true, this parameter must have a value.
Webserver Definition	default	optional	A web server definition allows for web server administration through the WebSphere administrative console. This parameter must be set if the Install Plugin parameter is set to true. An example would be webserver1. No spaces are allowed in the Webserver Definition name.
WebSphere Hostname	default	optional	Host name of the WebSphere Application Server machine. This parameter is required if Install Plugin is set to true. No spaces are allowed in the host name.

Additional Parameters Defined in this Step: Install IHS for WebSphere 7

Parameter Name	Default Value	Required	Description
Password	no default	required	The Windows Administrator password. Required for Windows.
Username	no default	required	This is the Windows Administrator user. Required for Windows.

Create StandAlone from Existing WebSphere 7 Install

Use this workflow to create a stand-alone profile on an existing WebSphere 7 installation.

A stand-alone application server works independently—it is not part of a cell and does not interact with a deployment manager. The stand-alone profile is not suitable for distributed application server environments.

This workflow uses the built-in profile management functions (manageprofiles) in IBM WebSphere Application Server version 7 to create a stand-alone profile on top of an existing installation.

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

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

Prerequisites for this Workflow

Be sure that the following prerequisites are satisfied before you run the Create StandAlone from Existing WebSphere 7 Install workflow:

1. This workflow requires unchallenged `sudo` access to a user (typically root) who can access all required files and directories.
2. Per the WebSphere 7 documentation, the following system libraries are required before provisioning IBM WebSphere Application Server version 7 on 64-bit Red Hat Linux:

Platform	Required Library
64-bit Red Hat Enterprise Linux version 5	compat-libstdc++-33-3.2.3-61 compat-db-4.2.52-5.1 libXp-1.0.0-8 compat-libstdc++- 296-2.96-138 rpm-build- 4.4.2-37.el5

   Make sure that these libraries exist on each target server before running this workflow. If newer versions of these libraries are available, you can install the newer versions.
3. This workflow will install WebSphere Application Server as root because of the following IBM documented limitations:
   - Creation of a Linux service for WebSphere Application Server
   - Native registration with the operating system
   - Port conflicts that may occur with other installations of WebSphere Application Server that are not registered with the operating system

   If there is a need to run as a non-root user after installation, you can run a recursive `chown` under the installation root and set owner permissions accordingly.

For more information about prerequisites for WebSphere 7, refer to the WebSphere 8 Product Documentation.

How this Workflow Works

This topic contains the following information about the Create StandAlone from Existing WebSphere 7 Install workflow:

Overview

This workflow does the following things in the order shown:

1. Prepares and validates all parameters and creates the call wrapper that will be used to execute commands within a WebSphere 7 environment
2. Creates a new response file
3. Creates a stand-alone profile
4. Starts the stand-alone WebSphere Application Server V7.0

Validation Checks Performed

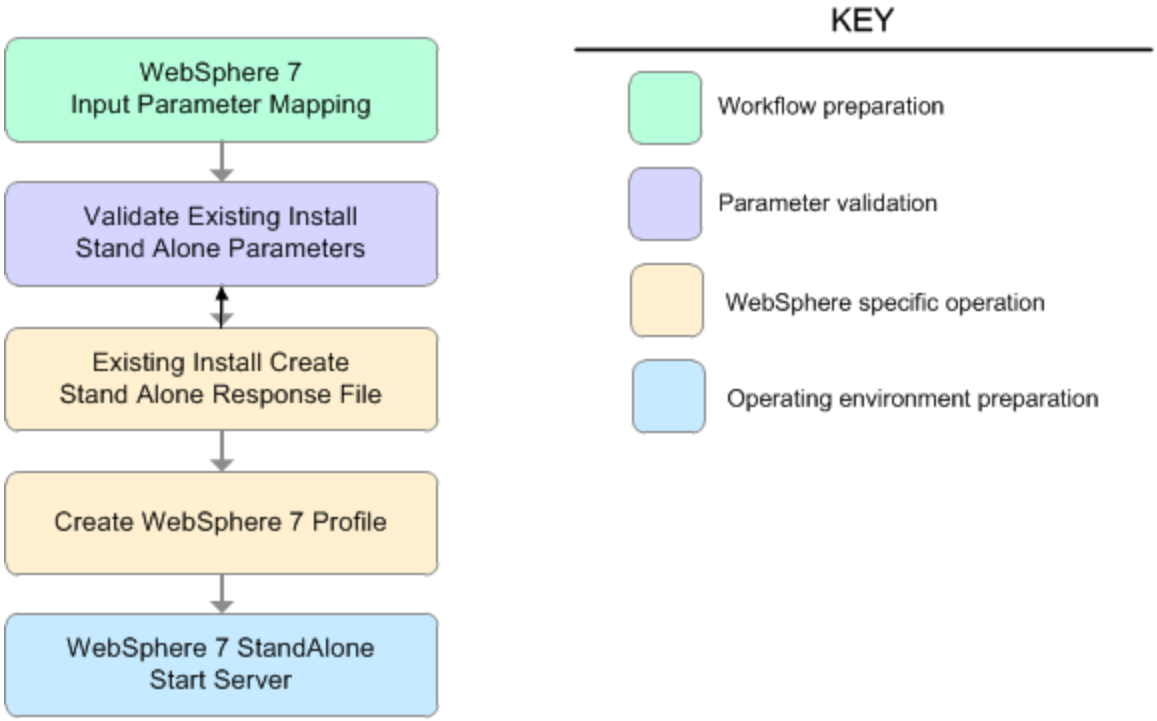
Most of the validation centers on special characters and spaces in the parameters. There are also validation checks that happen at the operating system level, including file system space checks and RPM checks for Red Hat Linux.

The workflow performs the following parameter checks:

1. Admin User (if specified) does not begin with a period (.), hyphen (-) or space. It does not contain any of the following characters: / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }
2. Admin Password (if specified) does not begin with a hyphen (-) or contain a space.
3. Cell Name, Node Name, Profile Name, and Server Name are specified. They do not contain the following characters: / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { } or space. They do not begin with a period.
4. Host Name is specified.
5. Default Ports and Developer Server (if specified) are true or false.
6. Enable Security is true or false. If Enable Security is true, Admin Password and Admin User are specified.
7. Omit Action (if specified) is defaultAppDeployAndConfig, or deployAdminConsole.
8. Ports File (if specified) exists and Validate Ports is true or false.
9. Starting Port (if specified) is an integer.
10. Profile Path and Response File are specified.
11. Install Location points to a valid existing WebSphere 7 installation.

Steps Executed

The Create StandAlone from Existing WebSphere 7 Install workflow includes the following steps. Each step must complete successfully before the next step can start. If a step fails, the workflow reports a failure, and all subsequent steps are skipped.



Steps Used in the Create StandAlone from Existing WebSphere 7 Install Workflow

Workflow Step	Description
WebSphere 7 Input Parameter Mapping	This step creates the call wrapper—the command that executes the step as a specific user—and allows certain parameters to be hidden or exposed.
Validate Existing Install Stand Alone Parameters	This step prepares and validates the parameters needed to create a stand-alone profile for an existing WebSphere Application Server V7.0 installation.
Existing Install Create Stand Alone Response File	This step creates a new response file to create a stand-alone profile on top of an existing WebSphere Application Server V7.0 installation.
Create WebSphere 7 Profile	This step creates a profile on top of an existing WebSphere Application Server V7.0 installation.
WebSphere 7 StandAlone Start Server	This step starts the stand-alone WebSphere Application Server V7.0.

Sample Scenario

This topic shows you typical parameter values used for the Create StandAlone from Existing WebSphere 7 Install workflow.

Stand-alone profile on Existing Install—Parameter Value Examples

Parameters Defined in this Step: Validate Existing Install Stand Alone Parameters

Parameter Name	Example Value	Description
Admin Password	wasPassWord	When Enable Security is set to true, this parameter must contain a string that does not begin with a dash(-) or contain a space( ).
Admin User	wasadmin	When Enable Security is set to true, this parameter must contain a string that does not begin with a dash(-), a period(.), or a space( ). It cannot contain any of the following characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }.
Cell Name	DevCell	Unique cell name that does not contain any of the following special characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }. If you plan to federate into an existing cell later, make sure that this name is not the same as the existing cell name.
Enable Security	true	Enables administrative security. Must be set to either true or false. If Enable Security is true, the Admin User and Admin Password parameters must have values.
Install Location	see description	Fully qualified path where WebSphere Application Server will be installed. For example: `/opt/IBM/WebSphere/AppServer`
Node Name	DevStandAlone1Node	Unique node name that cannot contain any of the following special characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }. If you plan to federate into an existing cell later, make sure that the name is unique within that cell.
Profile Name	StandAlone1	A unique profile name. It cannot begin with a period (.) and cannot contain any of the following special characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }.
Profile Path	see description	Fully qualifed path to the stand-alone profile. For example: `/opt/IBM/WebSphere/AppServer/profiles/AppServer1`
Response File	`/tmp/serverrsp`	Fully qualified path where the response file that this workflow creates will be located. This file will then be used to drive the installation and profile creation.
Server Name	Server1	Name of the application server that will be created under the profile.

How to Run this Workflow

The following instructions show you how to customize and run the Create StandAlone from Existing WebSphere 7 Install workflow in your environment.

The workflow provides default values for some parameters. These default values are usually sufficient for a "typical" installation. You can override the defaults by specifying parameter values in the deployment. You can also expose additional parameters in the workflow, if necessary, to accomplish more advanced scenarios. Any parameters not explicitly specified in the deployment will have the default values listed in "Parameters for Create StandAlone from Existing WebSphere 7 Install" on page 182

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

To customize and run the Create StandAlone from Existing WebSphere 7 Install workflow:

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

Input Parameters for Validate Existing Install Stand Alone Parameters

Parameter Name	Default Value	Required	Description
Admin Password	no default	optional	When Enable Security is set to true, this parameter must contain a string that does not begin with a dash(-) or contain a space( ).
Admin User	no default	optional	When Enable Security is set to true, this parameter must contain a string that does not begin with a dash(-), a period(.), or a space( ). It cannot contain any of the following characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }.
Cell Name	no default	required	Unique cell name that does not contain any of the following special characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }. If you plan to federate into an existing cell later, make sure that this name is not the same as the existing cell name.
Enable Security	no default	required	Enables administrative security. Must be set to either true or false. If Enable Security is true, the Admin User and Admin Password parameters must have values.
Install Location	no default	required	Fully qualified path where

Input Parameters for Validate Existing Install Stand Alone Parameters, continued

Parameter Name	Default Value	Required	Description
			WebSphere Application Server will be installed. For example: `/opt/IBM/WebSphere/AppServer`
Node Name	no default	required	Unique node name that cannot contain any of the following special characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }. If you plan to federate into an existing cell later, make sure that the name is unique within that cell.
Profile Name	no default	required	A unique profile name. It cannot begin with a period (.) and cannot contain any of the following special characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }.
Profile Path	no default	required	Fully qualifed path to the stand-alone profile. For example: `/opt/IBM/WebSphere/AppServer/profiles/AppServer1`
Response File	no default	required	Fully qualified path where the response file that this workflow creates will be located. This file will then be used to drive the installation and profile creation.
Server Name	no default	required	Name of the application server that will be created under the profile.

Additional Input Parameters for Install WebSphere 7 Create Profile

Parameter Name	Default Value	Required	Description
Password	no default	required	The Windows Administrator password. Required for Windows.
Username	no default	required	This is the Windows Administrator user. Required for Windows.

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

See "Parameters for Create StandAlone from Existing WebSphere 7 Install" on page 182 for detailed descriptions of all input parameters for this workflow, including default values.

> **Tip:** To avoid having to re-enter passwords whenever they change, you can create a policy to provide them to the workflow.

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

To verify the results:

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

Optional: if you want to further verify the results, perform the following steps:

1. After the workflow has completed, run the following command to check the version of WebSphere Application Server that was installed:

   WAS_ROOT/bin/versionInfo.sh

   Here, *WAS_ROOT* is the directory where WebSphere 7 is installed. This is the path that you specified in the WebSphere Install Location parameter.
2. Validate that stand-alone profile has been created and is running by doing the following:
   a. View the *WAS_ROOT*/profiles/*PROFILE_NAME*/logs/AboutThisProfile.txt file. This file is created after the creation of the profile and contains specific information about the profile.

      Here, *PROFILE_NAME* is the name of the profile that you just created. This is the name that you specified in the Profile Name parameter.

   b. Change to the *WAS_ROOT*/profiles/*PROFILE_NAME*/logs/*SERVER_NAME* directory, and tail the SystemOut.log file. Look for the following line:

      Server *SERVER_NAME* open for e-business

      Here, *SERVER_NAME* is the name of the application server that you just created. This is the name that you specified in the Server Name parameter.

Parameters for Create StandAlone from Existing WebSphere 7 Install

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

Parameters Defined in this Step: Validate Existing Install Stand Alone Parameters

Parameter Name	Default Value	Required	Description
Admin Password	no default	optional	When Enable Security is set to true, this parameter must contain a string that does not begin with a dash(-) or contain a space( ).
Admin User	no default	optional	When Enable Security is set to true, this parameter must contain a string that does not begin with a dash(-), a period(.), or a space( ). It cannot contain any of the following characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }.
Cell Name	no default	required	Unique cell name that does not contain any of the following special characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }. If you plan to federate into an existing cell later, make sure that this name is not the same as the existing cell name.
Default Ports	false	optional	Provides the option to assign default ports to a profile. Valid values are true or false. If true, the WebSphere Application Server default ports will be used, and the Ports File and Starting Port parameters should not have values. If false, the workflow will increment the default port until it finds a free port. The default value is false.
Developer Server	no default	optional	Use this parameter for development environments only to help with start up time. Valid value is true. Do not use in production environments.
Enable Security	no default	required	Enables administrative security. Must be set to either true or false. If Enable Security is true, the Admin User and Admin Password parameters must have values.
Host Name	Server.name	required	Hostname or IP address of the target machine.
Install Location	no default	required	Fully qualified path where WebSphere Application Server will be installed. For example: `/opt/IBM/WebSphere/AppServer`
Keystore Password	no default	optional	Sets the password for all keystore files created during profile creation. This includes keystore files for both the default personal certificate and the root signing certificate.
Node Name	no default	required	Unique node name that cannot contain any of the following special characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }. If you plan to federate into an existing cell later, make sure that the name is unique within that cell.

Parameters Defined in this Step: Validate Existing Install Stand Alone Parameters, continued

Parameter Name	Default Value	Required	Description
Omit Action	no default	optional	Enables you to prevent certain optional features from being installed. Valid values are deployAdminConsole or defaultAppDeployAndConfig. You may only specify one of these options.
Personal CertDN	no default	optional	Distinguished name of the personal certificate. For example: CN=dmalab-example.com,OU=WAS7LabCell, OU=WAS7LabDmgrManager,O=IBM,C=US The DN string cannot contain spaces. If you do not specify the DN, the WebSphere Application Server installer will create one.
Personal CertValidity Period	1	optional	Amount of time in years that the personal certificate is valid. Default is one year.
Ports File	no default	optional	Fully qualified path to a file that defines port settings for the new profile. This file must contain key=value pairs that specify a service name and a port number (for example: WC_ adminhost=9060). This option should be used with the Validate Ports option.
Profile Name	no default	required	A unique profile name. It cannot begin with a period (.) and cannot contain any of the following special characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }.
Profile Path	no default	required	Fully qualifed path to the stand-alone profile. For example: `/opt/IBM/WebSphere/AppServer/ profiles/AppServer1`
Response File	no default	required	Fully qualified path where the response file that this workflow creates will be located. This file will then be used to drive the installation and profile creation.
Server Name	no default	required	Name of the application server that will be created under the profile.
Signing CertDN	no default	optional	Distinguished name of the signing certificate. For example: CN=dmalab-example.com, OU=Root Certificate, OU=WAS7TestLabCell, OU=WAS7LabNode1, O=IBM, C=US The DN string cannot contain spaces. If you do not specify the DN, the WebSphere Application Server installer will create one.
Signing CertValidity Period	15	optional	Amount of time in years that the root certificate is valid. Default is 15 years.

Parameters Defined in this Step: Validate Existing Install Stand Alone Parameters, continued

Parameter Name	Default Value	Required	Description
Starting Port	no default	optional	Starting port number that the profile will use to generate and assign port values. Port values are assigned sequentially from the Starting Port. Do not specify this parameter if you specify Default Ports or Ports File.
Validate Ports	no default	optional	Indicates that the ports should be validated to ensure that they are not already in use. Valid values are true or false. You should use this option if you specify a Ports File.
Admin Password	no default	optional	When Enable Security is set to true, this parameter must contain a string that does not begin with a dash(-) or contain a space( ).

Additional Parameters Defined in this Step: Create WebSphere 7 Profile

Parameter Name	Default Value	Required	Description
Password	no default	required	The Windows Administrator password. Required for Windows.
Username	no default	required	This is the Windows Administrator user. Required for Windows.

Note: Only those parameters that are configurable in a standard deployment are listed here. Input parameters that must be mapped to output parameters of previous steps are not listed.

Create Custom Node from Existing WebSphere 7 Install

Use this workflow to create a custom profile on an existing WebSphere 7 installation.

A custom profile initially contains an empty node with no servers. The workflow can add (federate) the server to the pertinent cell when the profile is created, or you can add it later yourself.

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

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

Prerequisites for this Workflow

Be sure that the following prerequisites are satisfied before you run the Create Custom Node from Existing WebSphere 7 Install workflow:

1. This workflow requires unchallenged `sudo` access to a user (typically root) who can access all required files and directories.
2. Per the WebSphere 7 documentation, the following system libraries are required before provisioning IBM WebSphere Application Server version 7 on 64-bit Red Hat Linux:

Platform	Required Library
64-bit Red Hat Enterprise Linux version 5	compat-libstdc++-33-3.2.3-61 compat-db-4.2.52-5.1 libXp-1.0.0-8 compat-libstdc++- 296-2.96-138 rpm-build- 4.4.2-37.el5

   Make sure that these libraries exist on each target server before running this workflow. If newer versions of these libraries are available, you can install the newer versions.
3. This workflow will install WebSphere Application Server as root because of the following IBM documented limitations:
   - Creation of a Linux service for WebSphere Application Server
   - Native registration with the operating system
   - Port conflicts that may occur with other installations of WebSphere Application Server that are not registered with the operating system

   If there is a need to run as a non-root user after installation, you can run a recursive `chown` under the installation root and set owner permissions accordingly.

For more information about prerequisites for WebSphere 7, refer to the WebSphere 8 Product Documentation

How this Workflow Works

This topic contains the following information about the Create Custom Node from Existing WebSphere 7 Install workflow:

Overview

This workflow does the following things in the order shown:

1. Prepares and validates all parameters and creates the call wrapper that will be used to execute commands within a WebSphere 7 environment
2. Creates a new response file
3. Creates a custom node profile
4. Optionally federates the custom managed node profile into a Deployment Manager

Validation Checks Performed

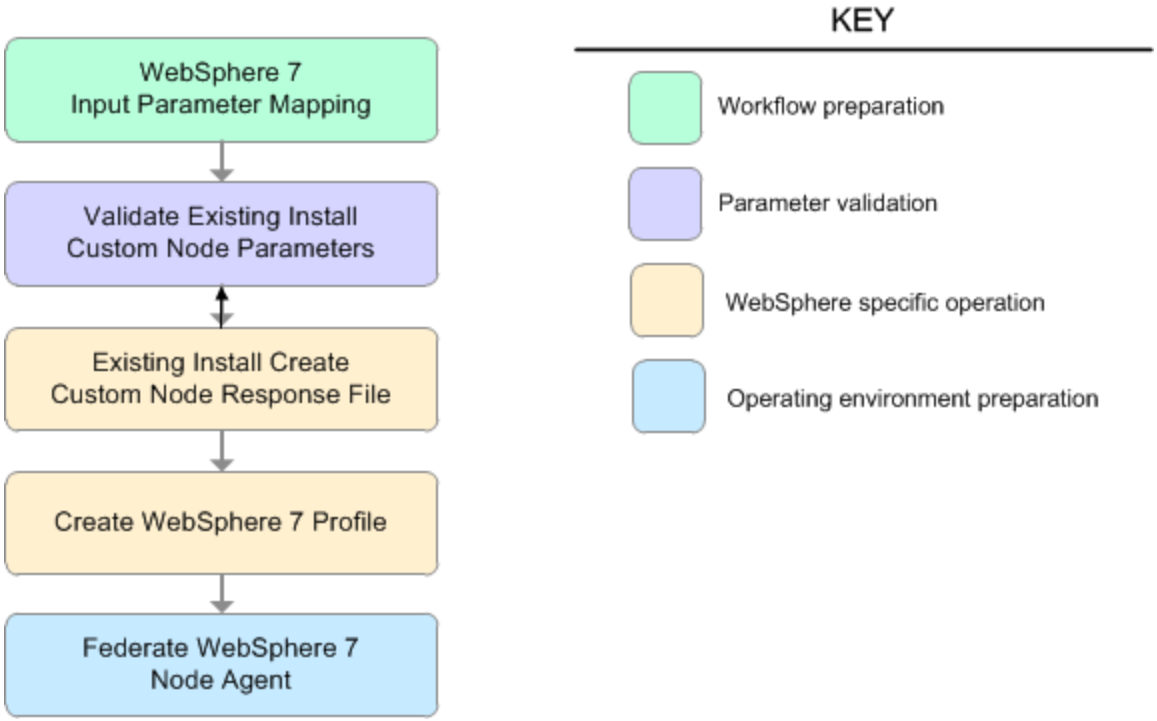
Most of the validation centers on special characters and spaces in the parameters. There are also validation checks that happen at the operating system level, including file system space checks and RPM checks for Red Hat Linux.

The workflow performs the following parameter checks:

1. Enable Security is true or false. If Enable Security is true, Dmgr Admin Password and Dmgr Admin User are specified.
2. Dmgr Admin User (if specified) does not begin with a period (.), hyphen (-) or space. It does not contain any of the following characters: / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }
3. Dmgr Admin Password (if specified) does not begin with a hyphen (-) or contain a space.
4. Cell Name, Node Name, and Profile Name are specified. They do not contain the following characters: / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { } or space. They do not begin with a period.
5. Host Name is specified.
6. Ports File (if specified) exists.
7. Federate Later (if specified) is true or false.
8. Dmgr Port (if specified) is an integer.
9. Profile Path and Response File are specified.
10. Install Location points to a valid existing WebSphere 7 installation.

Steps Executed

The Create Custom Node from Existing WebSphere 7 Install workflow includes the following steps. Each step must complete successfully before the next step can start. If a step fails, the workflow reports a failure, and all subsequent steps are skipped.



Steps Used in the Create Custom Node from Existing WebSphere 7 Install Workflow

Workflow Step	Description
WebSphere 7 Input Parameter Mapping	This step creates the call wrapper—the command that executes the step as a specific user—and allows certain parameters to be hidden or exposed.
Validate Existing Install Custom Node Parameters	This step prepares and validates the parameters needed to create a custom node profile for an existing WebSphere Application Server V7.0 installation.
Existing Install Create Custom Node Response File	This step creates a new response file to create a custom node profile on top of an existing WebSphere Application Server V7.0 installation.
Create WebSphere 7 Profile	This step creates a profile on top of an existing WebSphere Application Server V7.0 installation.

Steps Used in the Create Custom Node from Existing WebSphere 7 Install Workflow, continued

Workflow Step	Description
Federate WebSphere 7 Node Agent	This step federates the custom managed node profile into a Deployment Manager, creating a node agent.

Sample Scenario

This topic shows you typical parameter values used for the Create Custom Node from Existing WebSphere 7 Install workflow.

Add custom node profiles on existing WebSphere 7 install

Input Parameters for Validate Existing Install Custom Node Parameters

Parameter Name	Example Value	Description
Cell Name	Dev NodeCell	Unique cell name that does not contain any of the following special characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }. If you plan to federate into an existing cell later, make sure that this name is not the same as the existing cell name.
Dmgr Admin Password	wasPassWord	Administrative user password for the Deployment Manager. When Enable Security is set to true, this parameter must contain a string that does not begin with a dash(-) or contain a space( ).
Dmgr Admin User	wasadmin	Deployment Manager administrative user. When Enable Security is set to true, this parameter must contain a string that does not begin with a dash(-), a period(.), or a space( ). It cannot contain any of the following characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }.
Dmgr HostName	mycompany.com	Host name or IP address of the machine where the Deployment Manager is running. Specify this parameter and the Dmgr Port parameter to federate the new custom node as it is created. If you do not specify a value for this parameter, the new custom node is not federated (you must federate it later). Required if Federate Later is set to false.
Dmgr Port	8879	The SOAP port on which the Deployment Manager is listening. Specify this parameter and the Dmgr Host Name parameter to federate the new custom node as it is created. If you do not specify a value for this parameter, the new custom node is not federated (you must federate it later). Required if Federate Later is set to false.
Enable Security	true	Enables administrative security on the Deployment Manager. Must be set to either true or false. If Enable Security is true, the Dmgr Admin User and Dmgr Admin Password parameters must have values.
Install Location	see description	Fully qualified path where WebSphere Application Server will be installed. For example: `/opt/IBM/WebSphere/AppServer`
Node Name	DevNode	Unique node name that cannot contain any of the following special characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }. If you plan to federate into an existing cell later, make sure that the name is unique within that cell.
Profile Name	DevNode	A unique profile name. It cannot begin with a period (.) and cannot contain any of the following special characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }.

Input Parameters for Validate Existing Install Custom Node Parameters, continued

Parameter Name	Example Value	Description
Profile Path	see description	Fully qualifed path to the custom node profile. For example: `/opt/IBM/WebSphere/AppServer/profiles/ProdNode01`
Response File	`/tmp/serverrsp`	Fully qualified path where the response file that this workflow creates will be located. This file will then be used to drive the installation and profile creation.

Tip: To avoid having to re-enter passwords whenever they change, you can create a policy to provide them to the workflow.

How to Run this Workflow

The following instructions show you how to customize and run the Create Custom Node from Existing WebSphere 7 Install workflow in your environment.

The workflow provides default values for some parameters. These default values are usually sufficient for a "typical" installation. You can override the defaults by specifying parameter values in the deployment. You can also expose additional parameters in the workflow, if necessary, to accomplish more advanced scenarios. Any parameters not explicitly specified in the deployment will have the default values listed in "Parameters for Create Custom Node from Existing WebSphere 7 Install" on page 197

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

To customize and run the Create Custom Node from Existing WebSphere 7 Install workflow:

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

Input Parameters for Validate Existing Install Custom Node Parameters

Parameter Name	Default Value	Required	Description
Cell Name	no default	required	Unique cell name that does not contain any of the following special characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }. If you plan to federate into an existing cell later, make sure that this name is not the same as the existing cell name.
Dmgr Admin Password	no default	optional	Administrative user password for the Deployment Manager. When Enable Security is set to true, this parameter must contain a string that does not begin with a dash(-) or contain a space( ).
Dmgr Admin User	no default	optional	Deployment Manager administrative user. When Enable Security is set to true, this parameter must contain a string that does not begin with a dash(-), a period(.), or a space( ). It cannot contain any of the following characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }.
Dmgr HostName	no default	optional	Host name or IP address of the machine where the Deployment Manager is running. Specify this parameter and the Dmgr Port parameter to federate the new custom node as it is created. If you do not specify a value for this parameter, the new custom node is not federated (you must federate it later).

Input Parameters for Validate Existing Install Custom Node Parameters, continued

Parameter Name	Default Value	Required	Description
			Required if Federate Later is set to false.
Dmgr Port	no default	optional	The SOAP port on which the Deployment Manager is listening. Specify this parameter and the Dmgr Host Name parameter to federate the new custom node as it is created. If you do not specify a value for this parameter, the new custom node is not federated (you must federate it later). Required if Federate Later is set to false.
Enable Security	no default	required	Enables administrative security on the Deployment Manager. Must be set to either true or false. If Enable Security is true, the Dmgr Admin User and Dmgr Admin Password parameters must have values.
Install Location	no default	required	Fully qualified path where WebSphere Application Server will be installed. For example: `/opt/IBM/WebSphere/AppServer`
Node Name	no default	required	Unique node name that cannot contain any of the following special characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }. If you plan to federate into an existing cell later, make sure that the name is unique within that cell.
Profile Name	no default	required	A unique profile name. It cannot begin with a period (.) and cannot contain any of the following special characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }.
Profile Path	no default	required	Fully qualifed path to the custom node profile. For example: `/opt/IBM/WebSphere/AppServer/profiles/ProdNode01`
Response File	no default	required	Fully qualified path where the response file that this workflow creates will be located. This file will then be used to drive the installation and profile creation.

Additional Input Parameters for Install WebSphere 7 Create Profile

Parameter Name	Default Value	Required	Description
Password	no default	required	The Windows Administrator password. Required for Windows.
Username	no default	required	This is the Windows Administrator user. Required for Windows.

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

See "Parameters for Create Custom Node from Existing WebSphere 7 Install" on page 197 for detailed descriptions of all input parameters for this workflow, including default values.

Tip: To avoid having to re-enter passwords whenever they change, you can create a policy to provide them to the workflow.

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

To verify the results:

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

Optional: if you want to further verify the results, perform the following steps:

1. After the workflow has completed, run the following command to check the version of WebSphere Application Server that was installed:

   WAS_ROOT/bin/versionInfo.sh

   Here, *WAS_ROOT* is the directory where WebSphere 7 is installed. This is the path that you specified in the WebSphere Install Location parameter.
2. Validate that the Deployment Manager profile has been created and is running by doing the following:
   a. View the *WAS_ROOT*/profiles/*PROFILE_NAME*/logs/AboutThisProfile.txt file. This file is created after the creation of the profile and contains specific information about the profile.

      Here, *PROFILE_NAME* is the name of the profile that you just created. This is the name that you specified in the Profile Name parameter.

   b. Change to the *WAS_ROOT*/profiles/*PROFILE_NAME*/logs/nodeagent directory, and tail the SystemOut.log file. Look for the following line:

      Server nodeagent open for e-business

Parameters for Create Custom Node from Existing WebSphere 7 Install

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

Note: Only those parameters that are configurable in a standard deployment are listed here. Input parameters that must be mapped to output parameters of previous steps are not listed.

Parameters Defined in this Step: Validate Existing Install Custom Node Parameters

Parameter Name	Default Value	Required	Description
Cell Name	no default	required	Unique cell name that does not contain any of the following special characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }. If you plan to federate into an existing cell later, make sure that this name is not the same as the existing cell name.
Dmgr Admin Password	no default	optional	Administrative user password for the Deployment Manager. When Enable Security is set to true, this parameter must contain a string that does not begin with a dash(-) or contain a space( ).
Dmgr Admin User	no default	optional	Deployment Manager administrative user. When Enable Security is set to true, this parameter must contain a string that does not begin with a dash(-), a period(.), or a space( ). It cannot contain any of the following characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }.
Dmgr HostName	no default	optional	Host name or IP address of the machine where the Deployment Manager is running. Specify this parameter and the Dmgr Port parameter to federate the new custom node as it is created. If you do not specify a value for this parameter, the new custom node is not federated (you must federate it later). Required if Federate Later is set to false.
Dmgr Port	no default	optional	The SOAP port on which the Deployment Manager is listening. Specify this parameter and the Dmgr Host Name parameter to federate the new custom node as it is created. If you do not specify a value for this parameter, the new custom node is not federated (you must federate it later). Required if Federate Later is set to false.
Enable Security	no default	required	Enables administrative security on the Deployment Manager. Must be set to either true or false. If Enable Security is true, the Dmgr Admin User and Dmgr Admin Password parameters must have values.
Host Name	Server.name	required	Hostname or IP address of the target machine.
Install	no default	required	Fully qualified path where WebSphere Application Server will be

Parameters Defined in this Step: Validate Existing Install Custom Node Parameters, continued

Parameter Name	Default Value	Required	Description
Location			installed. For example: `/opt/IBM/WebSphere/AppServer`
Keystore Password	no default	optional	Sets the password for all keystore files created during profile creation. This includes keystore files for both the default personal certificate and the root signing certificate.
Node Name	no default	required	Unique node name that cannot contain any of the following special characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }. If you plan to federate into an existing cell later, make sure that the name is unique within that cell.
Personal CertDN	no default	optional	Distinguished name of the personal certificate. For example: CN=dmalab-example.com,OU=WAS7LabCell, OU=WAS7LabDmgrManager,O=IBM,C=US The DN string cannot contain spaces. If you do not specify the DN, the WebSphere Application Server installer will create one.
Personal CertValidity Period	1	optional	Amount of time in years that the personal certificate is valid. Default is one year.
Ports File	no default	optional	Fully qualified path to a file that defines port settings for the new profile. This file must contain key=value pairs that specify a service name and a port number (for example: WC_ adminhost=9060). This option should be used with the Validate Ports option.
Profile Name	no default	required	A unique profile name. It cannot begin with a period (.) and cannot contain any of the following special characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }.
Profile Path	no default	required	Fully qualifed path to the custom node profile. For example: `/opt/IBM/WebSphere/AppServer/ profiles/ProdNode01`
Response File	no default	required	Fully qualified path where the response file that this workflow creates will be located. This file will then be used to drive the installation and profile creation.
Signing CertDN	no default	optional	Distinguished name of the signing certificate. For example: CN=dmalab-example.com, OU=Root Certificate, OU=WAS7TestLabCell, OU=WAS7LabNode1, O=IBM, C=US The DN string cannot contain spaces. If you do not specify the DN, the WebSphere Application Server installer will create one.
Signing	15	optional	Amount of time in years that the root certificate is valid. Default

Parameters Defined in this Step: Validate Existing Install Custom Node Parameters, continued

Parameter Name	Default Value	Required	Description
CertValidity Period			is 15 years.

Additional Parameters Defined in this Step: Install WebSphere 7 Create Profile

Parameter Name	Default Value	Required	Description
Password	no default	required	The Windows Administrator password. Required for Windows.
Username	no default	required	This is the Windows Administrator user. Required for Windows.

Create and Configure WebSphere Data Sources

The purpose of this workflow is to create and configure a new WebSphere Application Server data source within the application server scope. This workflow creates the JDBC (Java Database Connectivity) provider, the J2C (Java 2 Connector) alias, and a data source associated with the JDBC provider.

Data sources—backend connections to an existing database—allow pooling of connections to the database for fast access, reuse by application components, and abstraction of the database connection information by WebSphere.

Supported vendors

The supported database vendors are:

- Oracle Database Enterprise Edition
- Microsoft SQL Server

The following chart shows shows the customizable parameters for WebSphere data sources:

Data source attribute	Configurable parameter
JDBC provider	Database Type (Oracle or SQL Server) Implementation Type (Connection pool source or XA data source) Provider Name Driver Class Path
J2C alias	J2C Alias Name Database User Name Database Password Description
Oracle data source	Oracle URL Java Name Directory Interface (JNDI) Name Data Source Name J2C Alias Name Minimum Pool Connections Maximum Pool Connections
SQL Server data source	Database Name Port Number DB Server Name JNDI Name Data Source Name J2C Alias Name Minimum Pool Connections Maximum Pool Connections

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

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

Prerequisites for this Workflow

Be sure that the following prerequisites are satisfied before you run the Create and Configure WebSphere Data Sources workflow.

Product Platform

This workflow is available for WebSphere 7.0, 8.0, or 8.5.x.

Dependencies

This workflow has the following dependencies:

- You must have a working WebSphere Network Deployment cell version 7.0, 8.0, or 8.5.x, with the Deployment Manager available for communication.
- You must run the Discover WebSphere workflow before you run the workflows. The Discover WebSphere workflow audits the server's physical environment for WebSphere cells, clusters, and application servers and stores the configuration information in the HPE DMA environment.
- You need either a working WebSphere Application Server (or servers) or cluster members associated with a cluster.
- You need a running Oracle or SQL Server backend database to connect the data source to.
- A compatible JDBC driver must be on the target machine (or machines). This is available from your database vendor.

  For example, a compatible driver for Oracle is `ojdbc6.jar` and for SQL Server is `sqljdbc4.jar`.

For more information about prerequisites for WebSphere, refer to the WebSphere 8 Product Documentation.

How this Workflow Works

The following information describes how the Create and Configure WebSphere Data Sources workflow works:

Overview

This workflow does the following things in the order shown:

1. Before creating the WebSphere data source, the workflow prepares and validates all parameters and creates the call wrapper that will be used to execute commands within a WebSphere environment.
2. Next the workflow stops the WebSphere Application Servers, uses the `AdminTask` command to create the data source according to all the user-specified options, and then restarts the WebSphere Application Servers.
3. Finally, the workflow verifies that the connection to the data source was successful and then discovers the WebSphere configurations associated with the data source.

Validation Checks Performed

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

WebSphere Admin Username	Cannot contain the following characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { } and also cannot begin with a dash (-), period (.), or space ( )
WebSphere Admin Password	Cannot begin with a dash (-) and cannot contain a space ( )
Enable Security	Must be true or false
If Enable Security is true	WebSphere Admin Username must be specified WebSphere Admin Password must be specified
Database Type	Must be either Oracle or SQL Server (case independent)
Database Type Database Password Database User Name Data Source Name Driver Class Path J2C Alias Name JNDI Name Provider Name	Must be specified
Implementation Type	Must be XA data source or Connection pool data source (case dependent)
If Database Type is Oracle	Oracle URL must be specified Database Name must be null Port Number must be null DB Server Name must be null
If Database Type is SQL Server	Database Name must be specified Port Number must be specified and be numeric DB Server Name must be specified Oracle URL must be null
Maximum Pool Connections Minimum Pool Connections	If specified, must be an integer
Web Service Password Web Service User	Must define a valid WebSphere cluster or application server

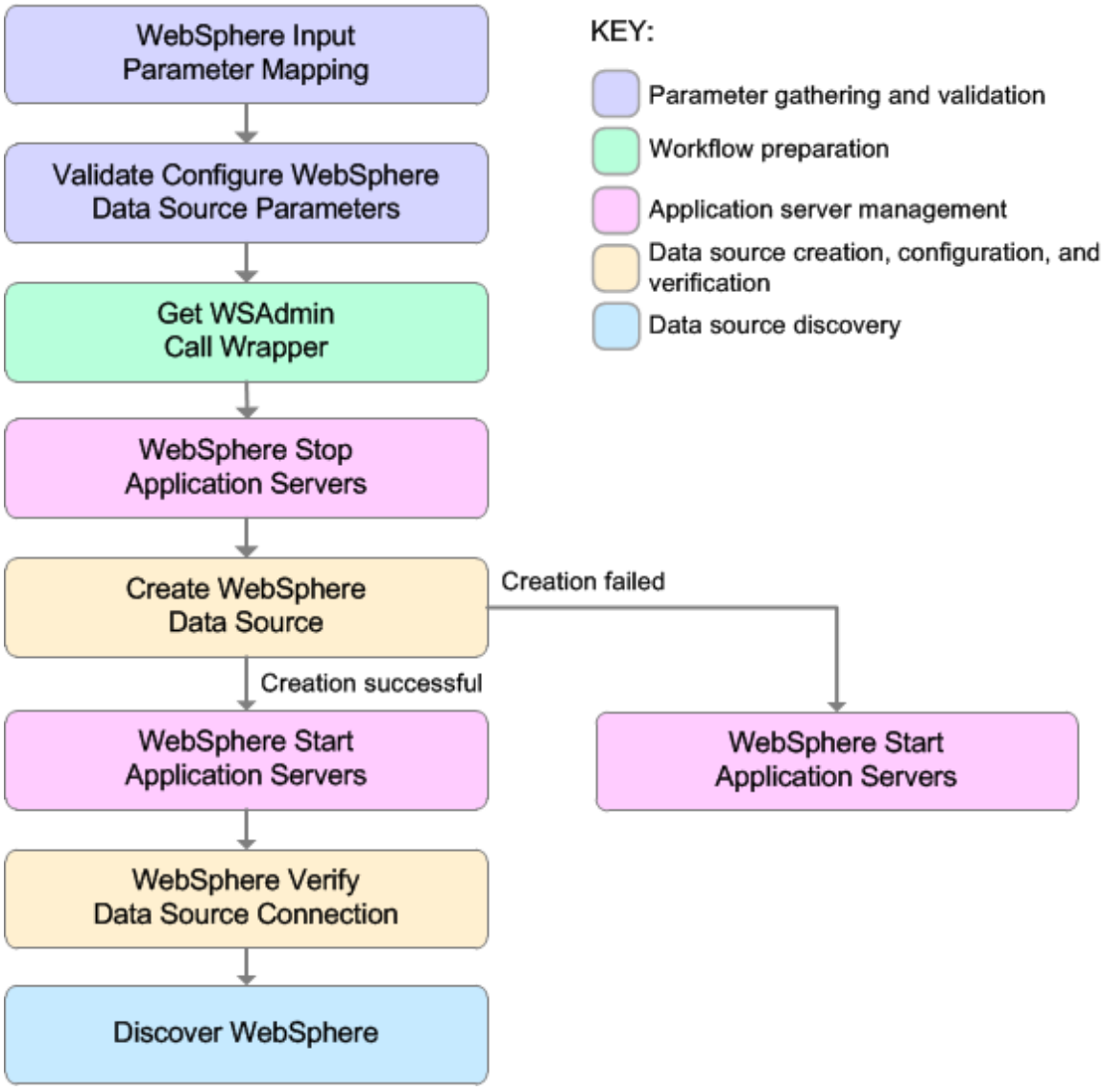
The Create and Configure WebSphere Data Sources workflow also checks the environment for the following:

- There needs to be valid organization, server ID, and instance IDs.
- The middleware platform must be WebSphere.
- There must be associated databases.
- The WebSphere container types must be Cluster or APPLICATION_SERVER.

Steps Executed

The Create and Configure WebSphere Data Sources workflow includes the following steps. Each step must complete successfully before the next step can start. If a step fails, the workflow reports a failure and all subsequent steps are skipped.

Click each box in the diagram to view additional information about that step.



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 HPE 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 220.

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 220.

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

To use the Create and Configure WebSphere Data Sources workflow:

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

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`
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.

Input Parameters for Validate Configure WebSphere Data Source Parameters , continued

Parameter Name	Default Value	Required	Description
Implementation Type	no default	required	The implementation type for the JDBC (Java Database Connectivity) provider. Use Connection pool data source if your application runs in a single phase or a local transaction. Otherwise, use XA data source to run in a global transaction. Valid values are Connection pool data source or XA data source.
J2C Alias Name	no default	required	Java 2 Connector (J2C) alias name. This will later be used for authentication purposes to map to the data source.
JNDI Name	no default	required	Java Name Directory Interface (JNDI) name. This is a user specified string specific to the application component calls to the data source. For example: `jdbc/myDatasource`
Oracle URL	no default	optional	Oracle URL for the data source to connect to the database. Only used if Database Type is set to Oracle. For example: `jdbc:oracle:thin:@//localhost:1521` for thin or `jdbc:oracle:oci:@//localhost:1521` for thick.
Port Number	no default	optional	The port number that the SQL Server database is listening on. Only used if Database Type is set to SQL Server.
Provider Name	no default	required	The name of the JDBC (Java Database Connectivity) provider. For example: My Oracle 11g JDBC Provider.
Trust SSL Certificates	no default	deprecated	HPE DMA no longer uses this workflow parameter to determine whether the workflow will trust any Secure Sockets Layer (SSL) certificate used to connect to the HPE DMA web service. HPE DMA uses the following parameter in the `dma.xml` file: `<Parameter name="com.hp.dma.conn. trustAllCertificates" values="VALUE" />` Here, VALUE is true or false.
Web Service Password	no default	required	Password for the HPE DMA Discovery web service API.
Web Service User	no default	required	A user capable of modifying the HPE DMA managed environment by using the web service API.
WebSphere Admin Password	no default	optional	The password for a user in a group that can change the state of a given application server. Only required if global security is enabled. It cannot not begin with a dash (-) or contain a space ( ).
WebSphere	no	optional	The user account for a user in a group that can change the

Input Parameters for Validate Configure WebSphere Data Source Parameters , continued

Parameter Name	Default Value	Required	Description
Admin Username	default		state of a given application server. Only required if global security is enabled. It cannot begin with a dash (-), a period (.), or a space ( ). It cannot contain any of the following characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }.

Tip: To avoid having to re-enter passwords whenever they change, you can create a policy to provide them to the workflow.

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

See "Parameters for Create and Configure WebSphere Data Sources" on page 220 for detailed descriptions of all input parameters for this workflow, including default values.

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

To verify the results:

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

Optional: If you want to further verify the results:

Use the WebSphere user interface to check that the data source is connected.

Sample Scenario

This topic shows you typical parameter values for different use cases for the Create and Configure WebSphere Data Sources workflow. For a complete list of all parameters used in this workflow, including default values, see "Parameters for Create and Configure WebSphere Data Sources" on page 220.

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

Tip: To avoid having to re-enter passwords whenever they change, you can create a policy to provide them to the workflow.

Scenario 1: To create an Oracle data source using connection pool data source

This use case will create an Oracle data source using connection pool data source. This example does not enable security.

Input Parameters for Validate Configure WebSphere Data Source Parameters

Parameter Name	Example Value	Description
Database Password	DbPassWord	Password for the database. It will be used for authentication purposes when connecting to the database in order to create the J2C alias.
Database Type	Oracle	The type of database that will be used by the JDBC (Java Database Connectivity) provider. Valid values are Oracle or SQL Server.
Database User Name	system	User name for the database. It will be used for authentication purposes when connecting to the database in order to create the J2C alias.
Data Source Name	Oracle App Data Source	The name given to the data source when it is created.
Driver Class Path	see description	A list of paths or JAR file names for the resource provider classes. For example: `/app/oracle/jdbc/ojdbc6.jar` for UNIX and `C:\app\oracle\jdbc\ojdbc6.jar` for Windows.
Enable Security	False	Indicates whether security will be enabled. Valid values are True or False. If True then WebSphere Admin Password and WebSphere Admin User must have values.
Implementation Type	Connection pool data source	The implementation type for the JDBC (Java Database Connectivity) provider. Use Connection pool data source if your application runs in a single phase or a local transaction. Otherwise, use XA data source to run in a global transaction. Valid values are Connection pool data source or XA data source.
J2C Alias Name	OraAppAlias	Java 2 Connector (J2C) alias name. This will later be used for authentication purposes to map to the data source.
JNDI Name	jdbc/	Java Name Directory Interface (JNDI) name. This is a user

Input Parameters for Validate Configure WebSphere Data Source Parameters , continued

Parameter Name	Example Value	Description
	oraAppDataSource	specified string specific to the application component calls to the data source. For example: `jdbc/myDatasource`
Oracle URL	see description	Oracle URL for the data source to connect to the database. Only used if Database Type is set to Oracle. For example: `jdbc:oracle:thin:@//localhost:1521` for thin or `jdbc:oracle:oci:@//localhost:1521` for thick.
Provider Name	Oracle App JDBC Provider	The name of the JDBC (Java Database Connectivity) provider. For example: My Oracle 11g JDBC Provider.
Web Service Password	myWebSvcPwd	Password for the HPE DMA Discovery web service API.
WebSphere Admin Password	JohnDoe	The password for a user in a group that can change the state of a given application server. Only required if global security is enabled. It cannot not begin with a dash (-) or contain a space ( ).

Scenario 2: To create an SQL Server data source using connection pool data source

This use case will create an SQL Server data source using connection pool data source and does not enable security.

Input Parameters for Validate Configure WebSphere Data Source Parameters

Parameter Name	Example Value	Description
Database Name	master	The name of the SQL Server database. Only used if Database Type 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/oracle/jdbc/ojdbc6.jar` for UNIX and `C:\app\oracle\jdbc\ojdbc6.jar` for Windows.
Enable Security	False	Indicates whether security will be enabled. Valid values are True or False. If True then WebSphere Admin Password and WebSphere Admin User must have values.
Implementation Type	Connection pool data source	The implementation type for the JDBC (Java Database Connectivity) provider. Use Connection pool data source if your application runs in a single phase or a local transaction. Otherwise, use XA data source to run in a global transaction. Valid values are Connection pool data source or XA data source.
J2C Alias Name	MSSQLAppAlias	Java 2 Connector (J2C) alias name. This will later be used for authentication purposes to map to the data source.
JNDI Name	jdbc/ sqlAppDataSource	Java Name Directory Interface (JNDI) name. This is a user specified string specific to the application component calls to the data source. For example: `jdbc/myDatasource`
Port Number	53074	The port number that the SQL Server database is listening on. Only used if Database Type is set to SQL Server.
Provider Name	MS SQL Server	The name of the JDBC (Java Database Connectivity) provider.

Input Parameters for Validate Configure WebSphere Data Source Parameters , continued

Parameter Name	Example Value	Description
	App JDBC Provider	For example: My Oracle 11g JDBC Provider.
Web Service Password	myWebSvcPwd	Password for the HPE DMA Discovery web service API.
WebSphere Admin Password	JohnDoe	The password for a user in a group that can change the state of a given application server. Only required if global security is enabled. It cannot not begin with a dash (-) or contain a space ( ).

Scenario 3: To create an Oracle data source using XA data source

This use case will create an Oracle data source using XA data source. To enable security you also need to specify WebSphere Admin Password and WebSphere Admin Username.

Input Parameters for Validate Configure WebSphere Data Source Parameters

Parameter Name	Example Value	Description
Database Password	DbPassWord	Password for the database. It will be used for authentication purposes when connecting to the database in order to create the J2C alias.
Database Type	Oracle	The type of database that will be used by the JDBC (Java Database Connectivity) provider. Valid values are Oracle or SQL Server.
Database User Name	system	User name for the database. It will be used for authentication purposes when connecting to the database in order to create the J2C alias.
Data Source Name	Oracle App XA Data Source	The name given to the data source when it is created.
Driver Class Path	see description	A list of paths or JAR file names for the resource provider classes. For example: `/app/oracle/jdbc/ojdbc6.jar` for UNIX and `C:\app\oracle\jdbc\ojdbc6.jar` for Windows.
Enable Security	True	Indicates whether security will be enabled. Valid values are True or False. If True then WebSphere Admin Password and WebSphere Admin User must have values.
Implementation Type	XA data source	The implementation type for the JDBC (Java Database Connectivity) provider. Use Connection pool data source if your application runs in a single phase or a local transaction. Otherwise, use XA data source to run in a global transaction. Valid values are Connection pool data source or XA data source.
J2C Alias Name	OraAppAlias	Java 2 Connector (J2C) alias name. This will later be used for authentication purposes to map to the data source.
JNDI Name	jdbc/ oraAppXADataSource	Java Name Directory Interface (JNDI) name. This is a user specified string specific to the application component calls to the data source. For example: `jdbc/myDatasource`
Oracle URL	see description	Oracle URL for the data source to connect to the database. Only used if Database Type is set to Oracle. For example: `jdbc:oracle:thin:@//localhost:1521` for thin or `jdbc:oracle:oci:@//localhost:1521` for thick.
Provider Name	Oracle App XA JDBC Provider	The name of the JDBC (Java Database Connectivity) provider. For example: My Oracle 11g JDBC Provider.

Input Parameters for Validate Configure WebSphere Data Source Parameters , continued

Parameter Name	Example Value	Description
Web Service Password	myWebSvcPwd	Password for the HPE DMA Discovery web service API.
Web Service User	JohnDoe	A user capable of modifying the HPE DMA managed environment by using the web service API.
WebSphere Admin Password	myPwd	The password for a user in a group that can change the state of a given application server. Only required if global security is enabled. It cannot not begin with a dash (-) or contain a space ( ).
WebSphere Admin Username	wasadmin	The user account for a user in a group that can change the state of a given application server. Only required if global security is enabled. It cannot begin with a dash (-), a period (.), or a space ( ). It cannot contain any of the following characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }.

Scenario 4: To create an SQL Server data source using XA data source

This use case will create an SQL Server data source using XA data source and specifying the Maximum and Minimum Pool Connections. This example does not enable security.

Note: Some of these parameters are not exposed by default in the deployment. You need to expose the following in the step Validate Configure WebSphere Data Source Parameters:

- Maximum Pool Connections
- Minimum Pool Connections

Input Parameters for Validate Configure WebSphere Data Source Parameters

Parameter Name	Example Value	Description
Database Name	master	The name of the SQL Server database. Only used if Database Type 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/oracle/jdbc/ojdbc6.jar` for UNIX and `C:\app\oracle\jdbc\ojdbc6.jar` for Windows.
Enable Security	False	Indicates whether security will be enabled. Valid values are True or False. If True then WebSphere Admin Password and WebSphere Admin User must have values.
Implementation Type	XA data source	The implementation type for the JDBC (Java Database Connectivity) provider. Use Connection pool data source if your application runs in a single phase or a local transaction. Otherwise, use XA data source to run in a global transaction. Valid values are Connection pool data source or XA data source.
J2C Alias Name	MSSQLAppAlias	Java 2 Connector (J2C) alias name. This will later be used for authentication purposes to map to the data source.

Input Parameters for Validate Configure WebSphere Data Source Parameters, continued

Parameter Name	Example Value	Description
JNDI Name	jdbc/ sqlAppXADataSource	Java Name Directory Interface (JNDI) name. This is a user specified string specific to the application component calls to the data source. For example: `jdbc/myDatasource`
Maximum Pool Connections	40	The maximum number of connections to be maintained in the data source connection pool. The default is the WebSphere default value.
Minimum Pool Connections	20	The minimum number of connections to be maintained in the data source connection pool. The default is the WebSphere default value.
Port Number	53074	The port number that the SQL Server database is listening on. Only used if Database Type is set to SQL Server.
Provider Name	MS SQL Server App XA JDBC Provider	The name of the JDBC (Java Database Connectivity) provider. For example: My Oracle 11g JDBC Provider.
Web Service Password	myWebSvcPwd	Password for the HPE DMA Discovery web service API.
Web Service User	JohnDoe	A user capable of modifying the HPE DMA managed environment by using the web service API.

Parameters for Create and Configure WebSphere Data Sources

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

Parameters Defined in this Step: Validate Configure WebSphere Data Source Parameters

Parameter Name	Default Value	Required	Description
Database Name	no default	optional	The name of the SQL Server database. Only used if Database Type 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.
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

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

Parameter Name	Default Value	Required	Description
			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.
Provider Type	no default	required	The JDBC (Java Database Connectivity) provider type. Valid values are Oracle JDBC Driver or Microsoft SQL Server JDBC Driver.
Trust SSL Certificates	no default	deprecated	HPE DMA no longer uses this workflow parameter to determine whether the workflow will trust any Secure Sockets Layer (SSL) certificate used to connect to the HPE DMA web service. HPE DMA uses the following parameter in the `dma.xml` file: `<Parameter name="com.hp.dma.conn. trustAllCertificates" values="VALUE" />` Here, VALUE is true or false.
Web Service Password	no default	required	Password for the HPE DMA Discovery web service API.
Web Service User	no default	required	A user capable of modifying the HPE DMA managed environment by using the web service API.
WebSphere Admin Password	no default	optional	The password for a user in a group that can change the state of a given application server. Only required if global security is enabled. It cannot not begin with a dash (-) or contain a space ( ).
WebSphere Admin	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

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

Parameter Name	Default Value	Required	Description
Username			security is enabled. It cannot begin with a dash (-), a period (.), or a space ( ). It cannot contain any of the following characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }.

Create and Configure WebSphere Web Server Definitions

The purpose of this workflow is to configure web server objects in a given WebSphere Application Server cell. These web server objects can be used later when deploying applications into a given application server or cluster. They also give limited ability to administer the web server instances.

First, the workflow creates an unmanaged node that represents the system where the web servers are running. Second, the workflow creates the web server definition under the unmanaged node. This node will hold information about the web server instance that runs on either the same machine or a remote machine.

Context

After the web server has been created an application can be installed and mapped to these web server objects at deployment time. Then a plug-in component can be generated based on the application configuration and application server information. The workflow consolidates that information into a single xml file that will be read by the web server plug-in.

Supported vendor

The supported web server vendor is IBM HTTP Server.

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

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

Prerequisites for this Workflow

Be sure that the following prerequisites are satisfied before you run the Create and Configure WebSphere Web Server Definitions workflow.

Product Platform

This workflow is available for WebSphere7.0, 8.0, or 8.5.x.

Dependencies

This workflow has the following dependencies:

- You must have a working WebSphere Network Deployment cell version 7.0, 8.0, or 8.5.x, with the Deployment Manager available for communication.
- You must run the Discover WebSphere workflow before you run the workflows. The Discover WebSphere workflow audits the server's physical environment for WebSphere cells, clusters, and application servers and stores the configuration information in the HPE DMA environment.

For more information about prerequisites for WebSphere, refer to the WebSphere 8 Product Documentation.

How this Workflow Works

The following information describes how the Create and Configure WebSphere Web Server Definitions workflow works:

Overview

This workflow does the following things in the order shown:

1. Before creating the WebSphere web server definitions, the workflow prepares and validates all parameters and creates the call wrapper that will be used to execute commands within a WebSphere environment .
2. Next the workflow uses the AdminTask command with all the user-specified options to create and configure the WebSphere unmanaged node and to create an IHS web server definition.Then the workflow synchronizes the node if it is enabled.
3. Finally, the workflow discovers the web server definitions associated with a WebSphere node.

Validation Checks Performed

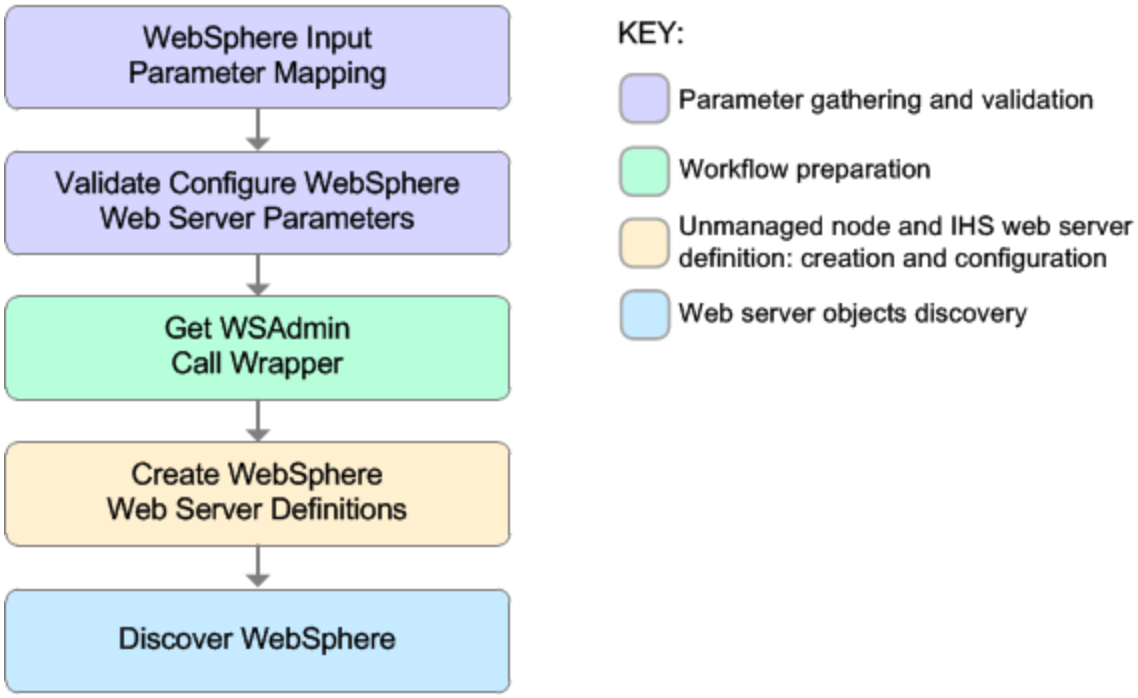
The workflow then performs the following checks on the input parameters:

Access Log File Error Log File HTTP Configuration File Plugin Install Root Web Server Install Root	Must be specified
Admin Protocol HTTP Web Protocol	If not specified, set to HTTP If specified, must be HTTP or HTTPS (case independent)
Unmanaged Node Host Name Unmanaged Node Name Web Server Name	Must be specified Cannot contain the following characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { } or space Cannot begin with a period (.)
HTTP Admin Password	Cannot begin with a dash (-) and cannot contain a space ( )
HTTP Admin User	Cannot contain the following characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { } and also cannot begin with a dash (-), period (.), or space ( )
HTTP Admin Port HTTP Web Port	Must be specified Must be an integer
Node Operating System	Must be aix, linux, solaris, or windows (case independent)
WebApp Mapping	If not specified, set to NONE If specified, must be ALL or NONE (case independent)
WebSphere Admin Username	Cannot contain the following characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { } and also cannot begin with a dash (-), period (.), or space ( )
WebSphere Admin Password	Cannot begin with a dash (-) and cannot contain a space ( )
Enable Security	Must be true or false
If Enable Security is true	WebSphere Admin Username must be specified WebSphere Admin Password must be specified
Web Service Password Web Service User	Must define a valid WebSphere Home

Steps Executed

The Create and Configure WebSphere Web Server Definitions workflow includes the following steps. Each step must complete successfully before the next step can start. If a step fails, the workflow reports a failure and all subsequent steps are skipped.

Click each box in the diagram to view additional information about that step.



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 HPE 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 236.

How to Run this Workflow

The following instructions show you how to customize and run the Create and Configure WebSphere Web Server Definitions workflow in your environment.

The workflow provides default values for some parameters. These default values are usually sufficient for a "typical" installation. You can override the defaults by specifying parameter values in the deployment.

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

To use the Create and Configure WebSphere Web Server Definitions workflow:

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

   Input Parameters for Validate Configure WebSphere Web Server Parameters

Parameter Name	Default Value	Required	Description
Access Log File	no default	required	Fully qualified path for the IBM HTTP Server access log file. For example: `/opt/IBM/HTTPServer/logs/access.log`
Admin Protocol	HTTP	optional	Administrative protocol title. Valid values are HTTP or HTTPS. The default is HTTP.
Enable Security	no default	required	Indicates whether security will be enabled. Valid values are True or False. If True then WebSphere Admin Password and WebSphere Admin User must have values.
Error Log File	no default	required	Fully qualified path for the IBM HTTP Server error log file. For example: `/opt/IBM/HTTPServer/logs/error.log`
HTTP Admin Password	no default	optional	Password for the HTTP Admin User.
HTTP Admin Port	8008	required	Port of the IBM HTTP Server administrative server.
HTTP Admin User	no default	optional	User name of the IBM HTTP administrative user.
HTTP Configuration File	no default	required	Fully qualified path for the IBM HTTP Server configuration file. For example: `/opt/IBM/HTTPServer/conf/httpd.conf`
HTTP Web Port	80	required	Port number of the IBM HTTP web server.
HTTP Web	HTTP	required	The protocol used by the IBM HTTP Server

Input Parameters for Validate Configure WebSphere Web Server Parameters, continued

Parameter Name	Default Value	Required	Description
Protocol			administrative server running with an unmanaged or remote web server. Valid values are HTTP or HTTPS. The default is HTTP.
Node Operating System	no default	required	The operating system in use on the system associated with the node specified in Unmanaged Node Name. Valid values are: aix, linux, solaris, windows.
Plugin Install Root	no default	required	The installation root directory where the plug-in for the web server is installed. For example: `/opt/IBM/HTTPServer/Plugin`
Service Name	no default	optional	The Windows service name for the IBM HTTP Server. Only required if the Node Operating System is Windows.
Trust SSL Certificates	no default	deprecated	HPE DMA no longer uses this workflow parameter to determine whether the workflow will trust any Secure Sockets Layer (SSL) certificate used to connect to the HPE DMA web service. HPE DMA uses the following parameter in the `dma.xml` file: `<Parameter name="com.hp.dma.conn. trustAllCertificates" values="VALUE" />` Here, VALUE is true or false.
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 HPE DMA Discovery web service API.
Web Service	no default	required	A user capable of modifying the HPE DMA managed

Input Parameters for Validate Configure WebSphere Web Server Parameters, continued

Parameter Name	Default Value	Required	Description
User			environment by using the web service API.
WebSphere Admin Password	no default	optional	The password for a user in a group that can change the state of a given application server. Only required if global security is enabled. It cannot not begin with a dash (-) or contain a space ( ).
WebSphere Admin Username	no default	optional	The user account for a user in a group that can change the state of a given application server. Only required if global security is enabled. It cannot begin with a dash (-), a period (.), or a space ( ). It cannot contain any of the following characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }.

Tip: To avoid having to re-enter passwords whenever they change, you can create a policy to provide them to the workflow.

Note: See "Parameters for Create and Configure WebSphere Web Server Definitions" on page 236 for detailed descriptions of all input parameters for this workflow, including default values.

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

To verify the results:

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

Optional: If you want to further verify the results:

Use the WebSphere administrative console interface to check that the web server is configured.

Sample Scenario

This topic shows you typical parameter values for different use cases for the Create and Configure WebSphere Web Server Definitions workflow. For a complete list of all parameters used in this workflow, including default values, see "Parameters for Create and Configure WebSphere Web Server Definitions" on page 236.

Tip: To avoid having to re-enter passwords whenever they change, you can create a policy to provide them to the workflow.

Scenario 1: To create and configure a WebSphere unmanaged node and web server definitions using unsecured protocol

This use case will create and configure a WebSphere unmanaged node and web server definitions using unsecured protocol. This example also does the following:

- Does not enable security
- Has the Linux operating system on the node
- Does not map any web applications to the web server

Input Parameters for Validate Configure WebSphere Web Server Parameters

Parameter Name	Example Value	Description
Access Log File	see description	Fully qualified path for the IBM HTTP Server access log file. For example: `/opt/IBM/HTTPServer/logs/access.log`
Admin Protocol	HTTP	Administrative protocol title. Valid values are HTTP or HTTPS. The default is HTTP.
Enable Security	False	Indicates whether security will be enabled. Valid values are True or False. If True then WebSphere Admin Password and WebSphere Admin User must have values.
Error Log File	see description	Fully qualified path for the IBM HTTP Server error log file. For example: `/opt/IBM/HTTPServer/logs/error.log`
HTTP Admin Password	HttpPassWoRd	Password for the HTTP Admin User.
HTTP Admin Port	8008	Port of the IBM HTTP Server administrative server.
HTTP Admin User	httpadmin	User name of the IBM HTTP administrative user.
HTTP Configuration File	see description	Fully qualified path for the IBM HTTP Server configuration file. For example: `/opt/IBM/HTTPServer/conf/httpd.conf`
HTTP Web Port	80	Port number of the IBM HTTP web server.
HTTP Web	HTTP	The protocol used by the IBM HTTP Server administrative server

Input Parameters for Validate Configure WebSphere Web Server Parameters, continued

Parameter Name	Example Value	Description
Protocol		running with an unmanaged or remote web server. Valid values are HTTP or HTTPS. The default is HTTP.
Node Operating System	linux	The operating system in use on the system associated with the node specified in Unmanaged Node Name. Valid values are: aix, linux, solaris, windows.
Plugin Install Root	see description	The installation root directory where the plug-in for the web server is installed. For example: `/opt/IBM/HTTPServer/Plugin`
Unmanaged Node Host Name	see description	Host name of the system associated with the node specified in Unmanaged Node Name. For example: `example.mycompany.com`
Unmanaged Node Name	webServerNode	The node name in the configuration repository.
WebApp Mapping	NONE	Level of installed web applications mapped to the web server. Valid values are ALL or NONE. The default is NONE.
Web Server Install Root	see description	Fully qualified directory path for the web server. For example: `/opt/IBM/HTTPServer`
Web Server Name	WebServer1	Name of the IBM HTTP web server.
Web Service Password	myWebSvcPwd	Password for the HPE DMA Discovery web service API.
Web Service User	JohnDoe	A user capable of modifying the HPE DMA managed environment by using the web service API.

Scenario 2: To create and configure a WebSphere unmanaged node and web server definitions using secured protocol

This use case will create and configure a WebSphere unmanaged node and web server definitions using unsecured protocol. This example also does the following:

- Enables security—WebSphere Admin Password and WebSphere Admin Username also need to be provided
- Has the AIX operating system on the node
- Maps all web applications to the web server

Input Parameters for Validate Configure WebSphere Web Server Parameters

Parameter Name	Example Value	Description
Access Log File	see description	Fully qualified path for the IBM HTTP Server access log file. For example: `/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.
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`

Input Parameters for Validate Configure WebSphere Web Server Parameters, continued

Parameter Name	Example Value	Description
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	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 HPE DMA Discovery web service API.
Web Service User	JohnDoe	A user capable of modifying the HPE DMA managed environment by using the web service API.
WebSphere Admin Password	myPwd	The password for a user in a group that can change the state of a given application server. Only required if global security is enabled. It cannot not begin with a dash (-) or contain a space ( ).
WebSphere Admin Username	wasadmin	The user account for a user in a group that can change the state of a given application server. Only required if global security is enabled. It cannot begin with a dash (-), a period (.), or a space ( ). It cannot contain any of the following characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }.

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.
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.

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

Parameter Name	Default Value	Required	Description
Trust SSL Certificates	no default	deprecated	HPE DMA no longer uses this workflow parameter to determine whether the workflow will trust any Secure Sockets Layer (SSL) certificate used to connect to the HPE DMA web service. HPE DMA uses the following parameter in the `dma.xml` file: `<Parameter name="com.hp.dma.conn. trustAllCertificates" values="VALUE" />` Here, VALUE is true or false.
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 HPE DMA Discovery web service API.
Web Service User	no default	required	A user capable of modifying the HPE DMA managed environment by using the web service API.
WebSphere Admin Password	no default	optional	The password for a user in a group that can change the state of a given application server. Only required if global security is enabled. It cannot not begin with a 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 / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }.

Configure WebSphere Cluster and Cluster Members

The purpose of this workflow is to create a new WebSphere Application Server cluster, create cluster members, and configure each cluster member.

The cluster members can be both vertically and horizontally clustered depending on the number of cluster members specified and the number of nodes that are within a cell.

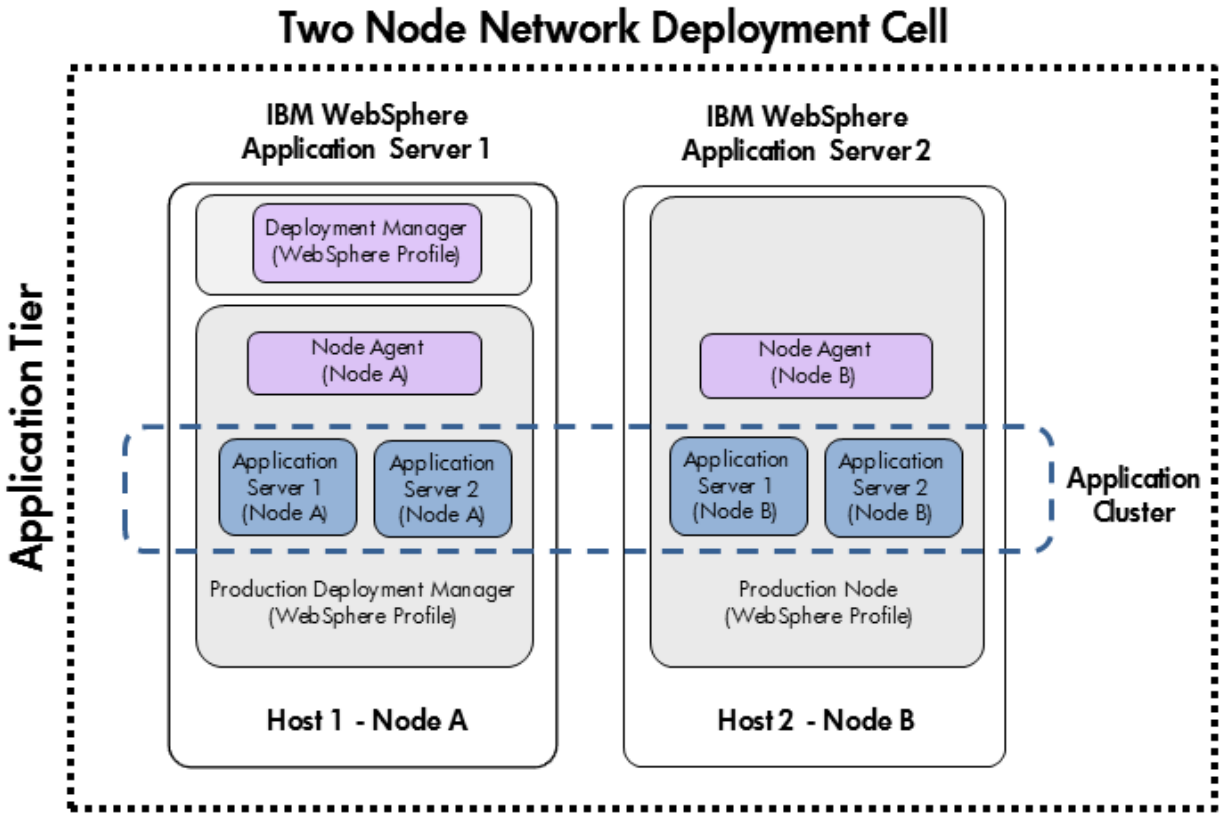
The cluster members are configured consistently based on a set of configurable parameters. If you do not specify parameters then the default WebSphere values are used.

The following chart shows the customizable parameters for WebSphere clusters and cluster members:

Cluster/cluster member attribute	**Configurable parameter**
Cluster definition	Cluster Name Cluster Member Name Number Cluster Members
Java Virtual Machine (JVM)	Initial Heap Size Maximum Heap Size
Logging	Logfile Location Rollover Type (SIZE, TIME, NONE, or BOTH) Base Hour Rollover Period Rollover Size Maximum Rollback Files

Architecture Diagram

The following is an example of a WebSphere Application Server environment:



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

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

Prerequisites for this Workflow

Be sure that the following prerequisites are satisfied before you run the Configure WebSphere Cluster and Cluster Members workflow.

Product Platform

This workflow is available for WebSphere7.0, 8.0, or 8.5.x.

Dependencies

This workflow has the following dependencies:

- You must have a working WebSphere Network Deployment cell version 7.0, 8.0, or 8.5.x, with the Deployment Manager available for communication.
- You must run the Discover WebSphere workflow before you run the workflows. The Discover WebSphere workflow audits the server's physical environment for WebSphere cells, clusters, and application servers and stores the configuration information in the HPE DMA environment.

For more information about prerequisites for WebSphere, refer to the WebSphere 8 Product Documentation.

How this Workflow Works

The following information describes how the Configure WebSphere Cluster and Cluster Members workflow works:

Overview

This workflow does the following things in the order shown:

1. Before creating the cluster and cluster members, the workflow prepares and validates all parameters and creates the call wrapper that will be used to execute commands within a WebSphere environment.
2. Next the workflow uses the call wrapper to call `wsadmin` to create the cluster and cluster members and to configure the cluster members.
3. Then the workflow starts the cluster to verify that it starts correctly and calls the component workflow, Discover WebSphere, to look for WebSphere configurations—including clusters and cluster members attributes.

Validation Checks Performed

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

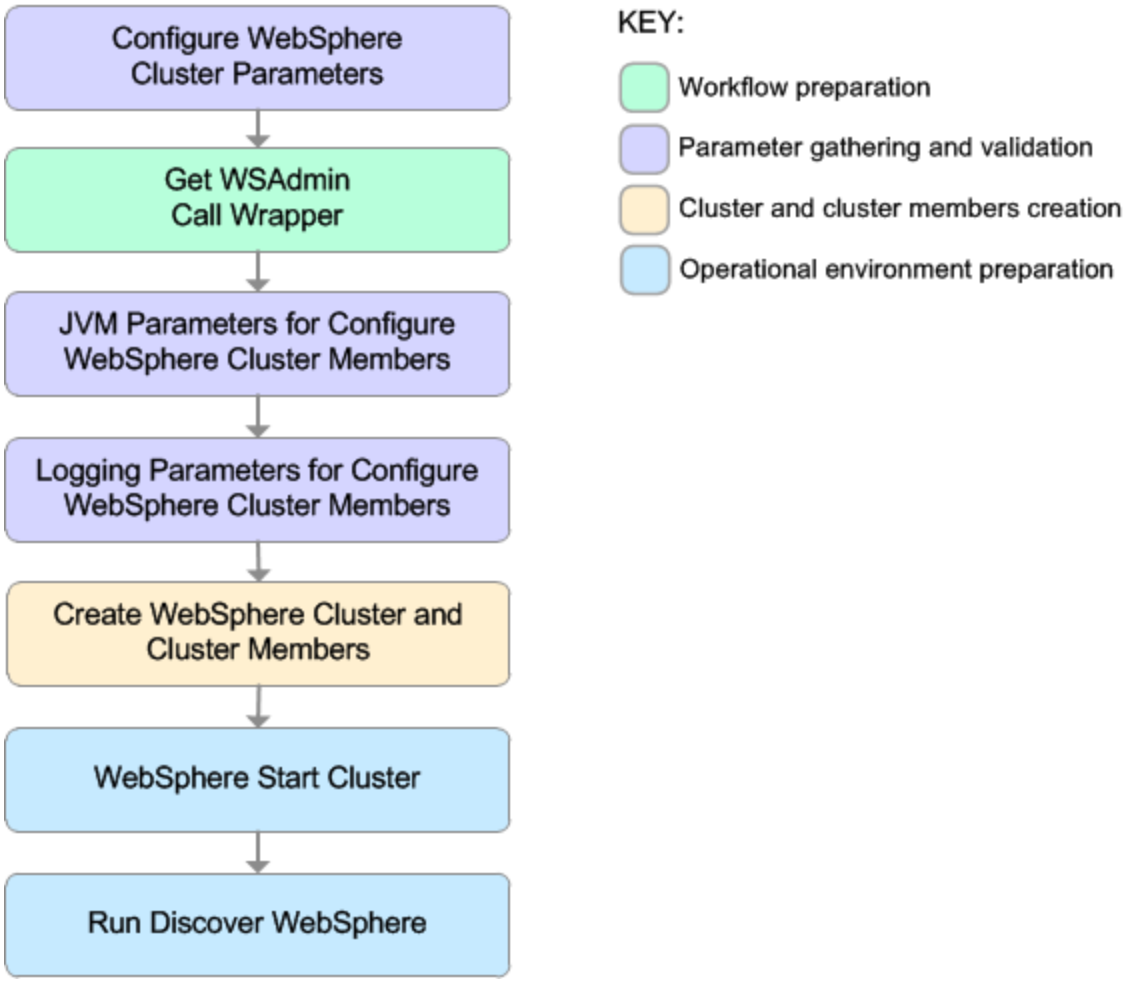
WebSphere Admin Username	Cannot contain the following characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { } and also cannot begin with a dash (-), period (.), or space ( )
WebSphere Admin Password	Cannot begin with a dash (-) and cannot contain a space ( )
Cluster Name Cluster Member Name	Must be specified Cannot contain the following characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { } 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	If one is specified the other must also be specified

Maximum Heap Size	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.

Click each box in the diagram to view additional information about that step.



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.

Steps Used in the Configure WebSphere Cluster and Cluster Members Workflow, continued

Workflow Step	Description
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 HPE 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 257.

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 257.

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

To use the Configure WebSphere Cluster and Cluster Members workflow:

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

   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.
Web Service Password	no	required	Password for the HPE DMA Discovery web

Input Parameters for Configure WebSphere Cluster Parameters, continued

Parameter Name	Default Value	Required	Description
	default		service API.
Web Service URL	no default	required	URL for the HPE DMA Discovery web service API. For example: `https://example.com:8443/dma`
Web Service User	no default	required	A user capable of modifying the HPE DMA managed environment by using the web service API.
WebSphere Admin Password	no default	optional	The password for a user in a group that can change the state of a given application server. Only required if global security is enabled. It cannot not begin with a dash (-) or contain a space ( ).
WebSphere Admin Username	no default	optional	The user account for a user in a group that can change the state of a given application server. Only required if global security is enabled. It cannot begin with a dash (-), a period (.), or a space ( ). It cannot contain any of the following characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }.

Tip: To avoid having to re-enter passwords whenever they change, you can create a policy to provide them to the workflow.

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

See "Parameters for Configure WebSphere Cluster and Cluster Members" on page 257 for detailed descriptions of all input parameters for this workflow, including default values.

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

To verify the results:

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

Sample Scenario

This topic shows you typical parameter values for different use cases for the Configure WebSphere Cluster and Cluster Members workflow. For a complete list of all parameters used in this workflow, including default values, see "Parameters for Configure WebSphere Cluster and Cluster Members" on page 257.

Tip: To avoid having to re-enter passwords whenever they change, you can create a policy to provide them to the workflow.

Scenario 1: To create two cluster members on each node using the default configurations

This use case will create a cluster testCluster with two nodes testApp001a and testApp001b. Security will be enabled. The WebSphere default values will be used for Initial Heap Size, Maximum Heap Size, and for logging.

Input Parameters for Configure WebSphere Cluster Parameters

Parameter Name	Example Value	Description
Cluster Member Name	testApp	The base cluster member name that will be used for each cluster member/application server. A suffix will automatically be appended to this base name that will indicate the node and cluster. For the initial cluster, the suffixes will be 001a for the first node, 001b for second node, and so on. If a vertical cluster member is created, the suffixes will be 002a for the first node, 002b for the second node, and so on. It cannot contain any of the following characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }.
Cluster Name	testCluster	This is the name given to the logical grouping of cluster members. This name has to be unique to the cell. It cannot contain any of the following characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }.
Enable Security	True	Indicates whether security will be enabled. Valid values are True or False. If True then WebSphere Admin Password and WebSphere Admin User must have values.
Number Cluster Members	2	The number of cluster members/application servers that will be created on each node.
Web Service Password	myWebSvcPwd	Password for the HPE DMA Discovery web service API.
Web Service URL	see description	URL for the HPE DMA Discovery web service API. For example: `https://example.com:8443/dma`
Web Service User	JohnDoe	A user capable of modifying the HPE DMA managed environment by using the web service API.
WebSphere	myPwd	The password for a user in a group that can change the state of a

Input Parameters for Configure WebSphere Cluster Parameters, continued

Parameter Name	Example Value	Description
Admin Password		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. 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 HPE DMA Discovery web service API.
Web Service URL	see description	URL for the HPE DMA Discovery web service API. For example: `https://example.com:8443/dma`
Web Service User	JohnDoe	A user capable of modifying the HPE DMA managed environment by using the web service API.
WebSphere Admin Password	myPwd	The password for a user in a group that can change the state of a given application server. Only required if global security is enabled. It cannot not begin with a dash (-) or contain a space ( ).

Input Parameters for Configure WebSphere Cluster Parameters, continued

Parameter Name	Example Value	Description
WebSphere Admin Username	wasadmin	The user account for a user in a group that can change the state of a given application server. Only required if global security is enabled. It cannot begin with a dash (-), a period (.), or a space ( ). It cannot contain any of the following characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }.

Input Parameters for JVM Parameters for Configure WebSphere Cluster Members

Parameter Name	Example Value	Description
Initial Heap Size	512	Initial heap size, in megabytes, that all cluster members will be set to on creation. The default is the WebSphere default value.
Maximum Heap Size	1024	Maximum heap size, in megabytes, that all cluster members will be set to on creation. The default is the WebSphere default value.

Scenario 3: To create two cluster members on each node, specifying initial and maximum heap sizes, and using a time-based logging configuration

This use case will create a cluster testCluster with two nodes testApp001a and testApp001b. The Initial Heap Size will be set to 512MB and the Maximum Heap Size to 1024MB. Security will not be enabled. The WebSphere periodic rollover logging will start at hour 1 (midnight), will update every 24 hours, and 7 historic logs will be saved.

Note: Some of these parameters are not exposed by default in the deployment. You need to expose the following:

In the step JVM Parameters for Configure WebSphere Cluster Members:

- Initial Heap Size
- Maximum Heap Size

In the step Logging Parameters for Configure WebSphere Cluster Members:

- Base Hour
- Logfile Location
- Maximum Rollback Files
- Rollover Period
- Rollover Type

Input Parameters for Configure WebSphere Cluster Parameters

Parameter Name	Example Value	Description
Cluster Member Name	testApp	The base cluster member name that will be used for each cluster member/application server. A suffix will automatically be appended to this base name that will indicate the node and cluster. For the initial cluster, the suffixes will be 001a for the first node, 001b for second node, and so on. If a vertical cluster member is created, the suffixes will be 002a for the first node, 002b for the second node, and so on. It cannot contain any of the following characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }.
Cluster Name	testCluster	This is the name given to the logical grouping of cluster members. This name has to be unique to the cell. It cannot contain any of the following characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }.
Enable Security	False	Indicates whether security will be enabled. Valid values are True or False. If True then WebSphere Admin Password and WebSphere Admin User must have values.
Number Cluster Members	2	The number of cluster members/application servers that will be created on each node.
Web Service Password	myWebSvcPwd	Password for the HPE DMA Discovery web service API.
Web	see description	URL for the HPE DMA Discovery web service API. For example:

Input Parameters for Configure WebSphere Cluster Parameters, continued

Parameter Name	Example Value	Description
Service URL		`https://example.com:8443/dma`
Web Service User	JohnDoe	A user capable of modifying the HPE DMA managed environment by using the web service API.

Input Parameters for JVM Parameters for Configure WebSphere Cluster Members

Parameter Name	Example Value	Description
Initial Heap Size	512	Initial heap size, in megabytes, that all cluster members will be set to on creation. The default is the WebSphere default value.
Maximum Heap Size	1024	Maximum heap size, in megabytes, that all cluster members will be set to on creation. The default is the WebSphere default value.

Input Parameters for Logging Parameters for Configure WebSphere Cluster Members

Parameter Name	Example Value	Description
Base Hour	1	The hour of the day, from 1 to 24, when the periodic rollover starts. The rollover always starts at the specified hour of the day. Hour 1 is 00:00:00 (midnight) and hour 24 is 23:00:00. Once started, the rollover repeats every Rollover Period hours.
Logfile Location	see description	Fully qualified directory path where the SystemOut and SystemErr logs will be created. For example: `/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. 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.
Web Service Password	myWebSvcPwd	Password for the HPE DMA Discovery web service API.
Web Service URL	see description	URL for the HPE DMA Discovery web service API. For example:

Input Parameters for Configure WebSphere Cluster Parameters, continued

Parameter Name	Example Value	Description
		`https://example.com:8443/dma`
Web Service User	JohnDoe	A user capable of modifying the HPE DMA managed environment by using the web service API.

Input Parameters for JVM Parameters for Configure WebSphere Cluster Members

Parameter Name	Example Value	Description
Initial Heap Size	512	Initial heap size, in megabytes, that all cluster members will be set to on creation. The default is the WebSphere default value.
Maximum Heap Size	1024	Maximum heap size, in megabytes, that all cluster members will be set to on creation. The default is the WebSphere default value.

Input Parameters for Logging Parameters for Configure WebSphere Cluster Members

Parameter Name	Example Value	Description
Logfile Location	see description	Fully qualified directory path where the SystemOut and SystemErr logs will be created. For example: `/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. 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 HPE DMA Discovery web service API.
Web Service URL	no default	required	URL for the HPE DMA Discovery web service API. For example: `https://example.com:8443/dma`
Web Service User	no default	required	A user capable of modifying the HPE DMA managed environment by using the web service API.
WebSphere Admin Password	no default	optional	The password for a user in a group that can change the state of a given application server. Only required if global security is enabled. It cannot not begin with a 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 / \ * , : ; = + ? | < > & % ' " [ ] # $

Parameters Defined in this Step: Configure WebSphere Cluster Parameters, continued

Parameter Name	Default Value	Required	Description
			^{}.

Additional Parameters Defined in this Step: JVM Parameters for Configure WebSphere Cluster Members

Parameter Name	Default Value	Required	Description
Initial Heap Size	see description	optional	Initial heap size, in megabytes, that all cluster members will be set to on creation. The default is the WebSphere default value.
Maximum Heap Size	see description	optional	Maximum heap size, in megabytes, that all cluster members will be set to on creation. The default is the WebSphere default value.

Additional Parameters Defined in this Step: Logging Parameters for Configure WebSphere Cluster Members

Parameter Name	Default Value	Required	Description
Base Hour	no default	optional	The hour of the day, from 1 to 24, when the periodic rollover starts. The rollover always starts at the specified hour of the day. Hour 1 is 00:00:00 (midnight) and hour 24 is 23:00:00. Once started, the rollover repeats every Rollover Period hours.
Logfile Location	no default	optional	Fully qualified directory path where the SystemOut and SystemErr logs will be created. For example: `/app/logs`
Maximum Rollback Files	no default	optional	The number of historical logs to keep.
Rollover Period	no default	optional	The number of hours after which the log file rolls over. Valid values range from 1 to 24. Only used if Rollover Type is TIME or BOTH.
Rollover Size	no default	optional	The maximum size of the log file in megabytes. When the file reaches this size, it rolls over. Only used if Rollover Type is SIZE or BOTH.
Rollover Type	no default	optional	Type of log rollover. Valid values are SIZE, TIME, NONE or BOTH. The default is SIZE.

WebSphere - Code Release

This workflow automates application deployments in IBM WebSphere. In addition to deployment automation, this workflow can update JVM Generic Arguments and JVM System Properties on the Web Server, and also provides install options for application deployments.

Some install options are provided as parameters for the workflow, or, users can specify install options within a file for each of the applications to be deployed (Note that user-specified parameter values take the highest precedence). This workflow provides application deployment verification by providing the URLs. For successful application deployments, verifications and a list of the applications are maintained in the history file. In cases of unsuccessful application deployments, the workflow rolls back the deployment and restores the last successfully deployed application (if any).

The supported applications are of type :

- .war files
- .ear files

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

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

Prerequisites for this Workflow

Be sure that the following prerequisites are satisfied before you run the WebSphere - Code Release workflow.

Product Platform

This workflow is available for WebSphere7.0, 8.0, or 8.5.x.

Dependencies

This workflow has the following dependencies:

- You must have a working WebSphere Network Deployment cell version 7.0, 8.0, or 8.5.x, with the Deployment Manager available for communication.
- You must run the Discover WebSphere workflow before you run the workflows. The Discover WebSphere workflow audits the server's physical environment for WebSphere cells, clusters, and application servers and stores the configuration information in the HPE DMA environment.

For more information about prerequisites for WebSphere, refer to the WebSphere 8 Product Documentation.

How this Workflow Works

The following information describes how the WebSphere - Code Release workflow works:

Overview

This workflow does the following things in the order shown:

1. Initially, the workflow inputs all parameters, set defaults for optional parameters, and validates all parameters. If input files do not exist in the specified locations, they are downloaded from the software repository. The workflow performs a checksum to verify that the archive files should be deployed in the Application Server on a standalone setup.
2. Next, the workflow creates the installation options and the call wrapper that will be used to execute commands within a WebSphere environment. The workflow updates the JVM setting and then creates a backup. The workflow deploys the specified Application Archive files in the Application Server on a standalone setup.
3. If the application deployment succeeds, the workflow tests the URLs for the web servers and copies the application archives.
4. If the application deployment fails, the workflow rolls back the deployment and restores the last successfully deployed application (if any).
5. Finally, the workflow cleans up downloaded files based on the Cleanup on Success and Cleanup on Failure parameters.

Validation Checks Performed

The workflow performs the following checks on the input parameters:

Enable Security	Must be true or false
If Enable Security is true	WebSphere Admin Username must be specified WebSphere Admin Password must be specified
WebSphere Admin Username	Cannot contain the following characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { } and also cannot begin with a dash (-), period (.), or space ( )
WebSphere Admin Password	Cannot begin with a dash (-) and cannot contain a space ( )
Code Release Staging Location Code Release History Location	Must be valid absolute paths Cannot have the same values
Application Archive File List Md5 Checksum	There must be a checksum for each Application Archive file The Application Archive files must be type `.ear` or `.war` and have valid absolute paths Checksums must be valid hexadecimal numbers

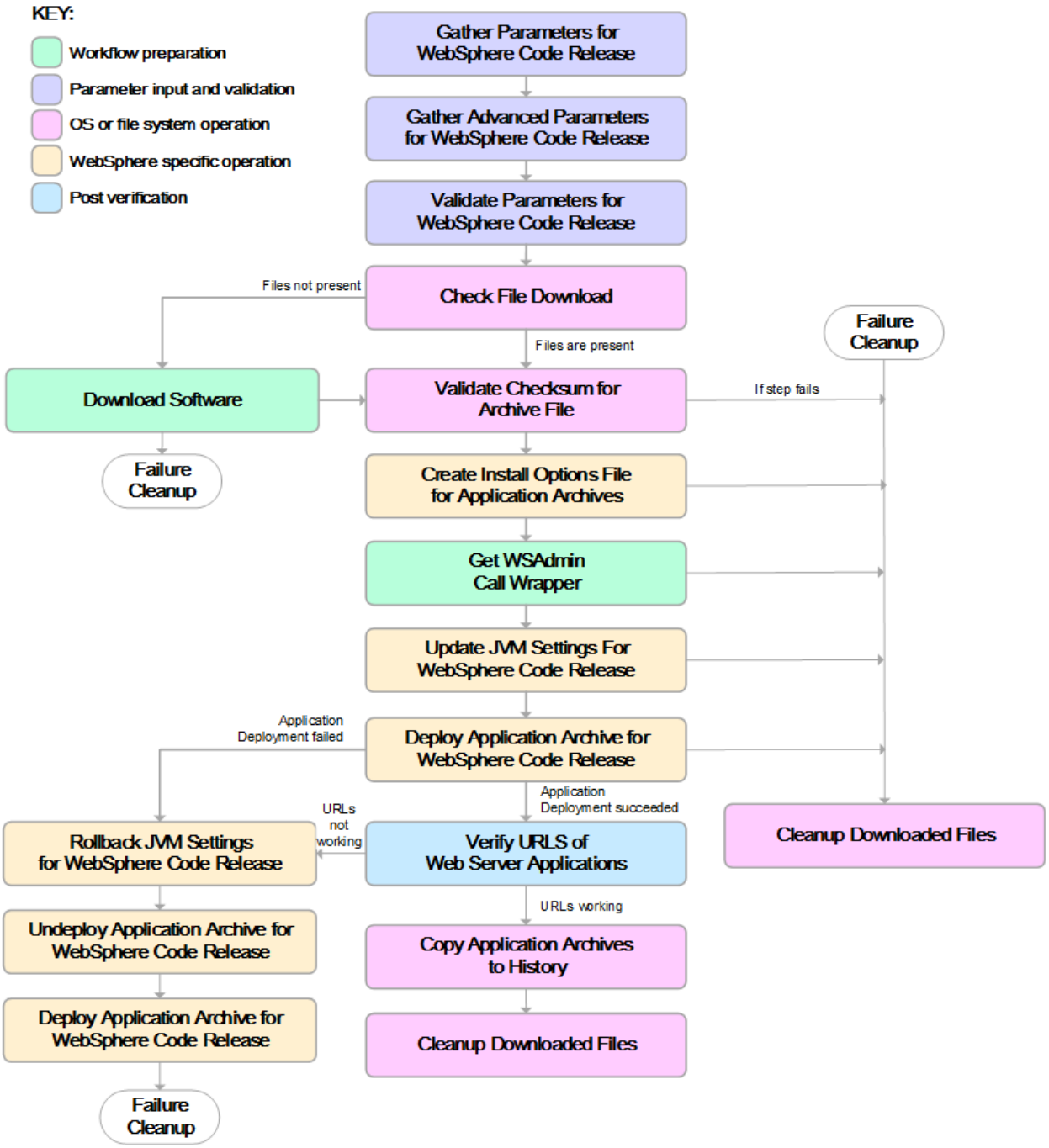
The WebSphere - Code Release workflow also checks the environment for the following:

- The WebSphere container type must be APPLICATION_SERVER.
- The WebSphere Home exists.

Steps Executed

The WebSphere - Code Release workflow includes the following steps. Each step must complete successfully before the next step can start. If a step fails, the workflow reports a failure and subsequent steps are skipped, except for the Cleanup Downloaded Files step.

Click each box in the diagram to view additional information about that step.



Steps Used in the WebSphere - Code Release Workflow

Workflow Step	Description
Gather Parameters for WebSphere Code Release	This step gathers mandatory input parameters (user-provided) used to deploy a list of application archives in a IBM WebSphere Application Server on a standalone setup.
Gather Advanced Parameters for WebSphere Code Release	This step gathers the advanced input parameters (user-provided) used to deploy an application archive for a WebSphere Application Server. Input parameters specified in this step are optional. Appropriate default values are specified.
Validate Parameters for WebSphere Code Release	This step validates the basic and advanced parameters provided by the user, and checks the prerequisites for deploying a list of application archives for an IBM WebSphere Application Server on a standalone setup.
Check File Download	This step checks for the existence of a file before downloading from the HP Server Automation software repository. • Checks if file is in the expected location. • If the file is not in the expected location, generates a list of files for file download.
Download Software	This step downloads a list of files to a specified location on the target server.
Validate Checksum for Archive File	This step verifies the checksum for the archive files and archive setting file (if any) to ensure that the file has not changed and that the correct archives are deployed in the Application Server.
Create Install Options File for Application Archives	This step creates a setting file that includes the install options for the list of application archive files being deployed by the application server.
Get WSAdmin Call Wrapper	This step creates the necessary call wrapper to call `wsadmin` to execute certain operations within a given WebSphere environment.
Update JVM Settings For WebSphere Code Release	This step updates the JVM setting of the IBM WebSphere Application server. It also performs a backup of the IBM WebSphere profile configuration.
Deploy Application Archive for WebSphere Code Release	Using the user-provided Application Archive files: This step deploys the list of application archives in the IBM WebSphere Application Server on a standalone setup.
If the application deployment succeeds, the following steps are executed	
Verify URLS of Web Server Applications	This step verifies that the URLs are working, and looks for return status code values of 200 for success.
Copy Application Archives to History	This step copies the list of files from the staging location to the history location.

Steps Used in the WebSphere - Code Release Workflow, continued

Workflow Step	Description
Cleanup Downloaded Files	For workflow success—and if Cleanup on Success is set to True (default)—this step removes all downloaded files and archives. Dependencies: Run as file/directory owner.
If the application deployment fails, the following steps are executed	
Rollback JVM Settings for WebSphere Code Release	This step restores a backup of the IBM WebSphere profile configuration.
Undeploy Application Archive for WebSphere Code Release	This step uninstalls the list of application archives from an IBM WebSphere Application Server on a standalone setup.
Deploy Application Archive for WebSphere Code Release	Using the backup of the Application Archive files: This step deploys the list of application archives in the IBM WebSphere Application Server on a standalone setup.
Cleanup Downloaded Files	For workflow failure—and if Cleanup on Failure is set to True (default)—this step removes all downloaded files and archives. Dependencies: Run as file/directory owner.

For parameter descriptions and defaults, see "Parameters for WebSphere - Code Release" on page 269.

How to Run this Workflow

The following instructions show you how to customize and run the WebSphere - Code Release workflow in your environment.

The workflow provides default values for some parameters. These default values are usually sufficient for a "typical" installation. You can override the defaults by specifying parameter values in the deployment.

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

To use the WebSphere - Code Release workflow:

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

   Parameters Defined in this Step: Gather Parameters for WebSphere - Code Release

Parameter Name	Default Value	Required	Description
Application	no default	required	Comma-separated list of the Application Archive files to

Parameters Defined in this Step: Gather Parameters for WebSphere - Code Release , continued

Parameter Name	Default Value	Required	Description
Archive File List			be deployed. Example: xxx.war or yyy.ear
Code Release History Location	no default	required	Fully qualified path name of the location where the application archive will be saved (for history purposes) on the target machine. This location cannot be the same as the Code Release Staging Location.
Code Release Staging Location	no default	required	Fully qualified path name of the location where the application archive will be saved on the target machine. This location cannot be the same as the Code Release History Location.
Enable Security	no default	required	Indicates whether security will be enabled. Valid values are True or False. If True then WebSphere Admin Password and WebSphere Admin User must have values.
MD5 Checksum	no default	required	Comma-separated list of the MD5 Checksum of the Application Archive files to be deployed.
Test URLs	no default	required	Comma-separated list of URLs used to test whether or not the list of applications deployed successfully. Example: http://mytestdb.com, http://yourtest.com

Tip: To avoid having to re-enter passwords whenever they change, you can create a policy to provide them to the workflow.

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

See "Parameters for WebSphere - Code Release" on page 269 for detailed descriptions of all input parameters for this workflow, including default values.

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

To verify the results:

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

Optional: If you want to further verify the results:

Use the WebSphere administrative console interface to check that the web server is configured.

Sample Scenario

This topic shows you typical parameter values for different use cases for the WebSphere - Code Release workflow. For a complete list of all parameters used in this workflow, including default values, see "Parameters for WebSphere - Code Release" on page 269.

Tip: To avoid having to re-enter passwords whenever they change, you can create a policy to provide them to the workflow.

Scenario 1: Install an application archive (for example stocksanalysis.war) on a running IBM WebSphere Application Server on a standalone setup.

In this scenario we will deploy the stockanalysis.war file on a running IBM WebSphere Application Server. We will install the application using the default installation options. If the application archive files are not present in the Code Release Staging Location, then they will be downloaded from the SA Repository.

Parameters Defined in this Step: Gather Parameters for WebSphere - Code Release

Parameter Name	Example Value	Description
Application Archive File List	stockanalysis.war	Comma-separated list of the Application Archive files to be deployed. Example: xxx.war or yyy.ear
Code Release History Location	/opt/IBM/was/history	Fully qualified path name of the location where the application archive will be saved (for history purposes) on the target machine. This location cannot be the same as the Code Release Staging Location.
Code Release Staging Location	/tmp/IBM/was/staging	Fully qualified path name of the location where the application archive will be saved on the target machine. This location cannot be the same as the Code Release History Location.
Enable Security	False	Indicates whether security will be enabled. Valid values are True or False. If True then WebSphere Admin Password and WebSphere Admin User

Parameters Defined in this Step: Gather Parameters for WebSphere - Code Release , continued

Parameter Name	Example Value	Description
		must have values.
MD5 Checksum	4477e994e9d457ad2214a3d36b1bb16b	Comma-separated list of the MD5 Checksum of the Application Archive files to be deployed.
Test URLs	http://<server:port>/stockanalysis/<xyx.html>	Comma-separated list of URLs used to test whether or not the list of applications deployed successfully. Example: http://mytestdb.com, http://yourtest.com

Scenario 2: Install an application archive (for example stocksanalysis.war) on a running IBM WebSphere Application Server on a standalone setup.

In this scenario we will deploy the stockanalysis.war file on a running IBM WebSphere Application Server. We will install the application using the default installation options. The JVM settings are also applied to the Application server. If the application archive files are not present in the Code Release Staging Location, then they will be downloaded from the SA Repository.

Parameters Defined in this Step: Gather Parameters for WebSphere - Code Release

Parameter Name	Example Value	Description
Application Archive File List	stockanalysis.war	Comma-separated list of the Application Archive files to be deployed. Example: xxx.war or yyy.ear
Code Release History Location	/opt/IBM/was/history	Fully qualified path name of the location where the application archive will be saved (for history purposes) on the target machine. This location cannot be the same as the Code Release Staging Location.
Code Release Staging Location	/tmp/IBM/was/staging	Fully qualified path name of the location where the application archive will be saved on the target machine. This location cannot be the same as the Code Release History Location.
Enable Security	False	Indicates whether security will be enabled. Valid values are True or False. If True then WebSphere Admin Password and WebSphere Admin User must have values.

Parameters Defined in this Step: Gather Parameters for WebSphere - Code Release , continued

Parameter Name	Example Value	Description
MD5 Checksum	4477e994e9d457ad2214a3d36b1bb16b	Comma-separated list of the MD5 Checksum of the Application Archive files to be deployed.
Test URLs	http://<server:port>/stockanalysis/<xyx.html>	Comma-separated list of URLs used to test whether or not the list of applications deployed successfully. Example: http://mytestdb.com, http://yourtest.com

Parameters Defined in this Step: Gather Advanced Parameters for WebSphere - Code Release

Parameter Name	Example Value	Description
JVM Generic Arguments	• Dclient.encoding.override=UTF-8 • Dsun.rmi.dgc.client.gcInterval=3600000000 • Dsun.rmi.dgc.server.gcInterval=3600000000	Specifies the JVM generic arguments. Provide values as standard JVM settings.
JVM System Properties	stockanalysis _home, /opt/stockanalysis/bin, Home path for the stock analysis	Specifies the JVM System Properties. Provide the string in the following format: 'PropertyName, PropertyValue||PropertyName, PropertyValue'

Scenario 3: Install an application archive (for example stocksanalysis.war) on a running IBM WebSphere Application Server on a standalone setup.

In this scenario we deploy the stockanalysis.war file on a running IBM WebSphere Application Server. We will install the application using the default installation options. This scenario provides the install options to deploy the application archive in a file. If the Application Archive Files and the Archive Setting File are not present in the Code Release Staging Location, then they will be downloaded from the SA Repository.

Parameters Defined in this Step: Gather Parameters for WebSphere - Code Release

Parameter Name	Example Value	Description
Application Archive File List	stockanalysis.war	Comma-separated list of the Application Archive files to be deployed. Example: xxx.war or yyy.ear
Code Release History Location	/opt/IBM/was/history	Fully qualified path name of the location where the application archive will be saved (for history purposes) on the target machine. This location cannot be the same as the Code Release Staging Location.

Parameters Defined in this Step: Gather Parameters for WebSphere - Code Release , continued

Parameter Name	Example Value	Description
Code Release Staging Location	/tmp/IBM/was/staging	Fully qualified path name of the location where the application archive will be saved on the target machine. This location cannot be the same as the Code Release History Location.
Enable Security	False	Indicates whether security will be enabled. Valid values are True or False. If True then WebSphere Admin Password and WebSphere Admin User must have values.
MD5 Checksum	4477e994e9d457ad2214a3d36b1bb16, 1eff908bedaa416c104f6b4a9a268233	Comma-separated list of the MD5 Checksum of the Application Archive files to be deployed.
Test URLs	http://<server:port>/stock/<xyx.html>	Comma-separated list of URLs used to test whether or not the list of applications deployed successfully. Example: http://mytestdb.com, http://yourtest.com

Parameters Defined in this Step: Gather Advanced Parameters for WebSphere - Code Release

Parameter Name	Example Value	Description

Archive Settings File	archive.setting	The file containing the install options for all the archive files.
		Sample Archive Settings File content:
		`stockanalysis.war = {`
		`Precompile JavaServer Pages files = No`
		`-contextroot /stock`
		`}`
		Options for providing the key are:
		• Provide the key in plain English. The key supported is the parameter name in the step Gather Advanced Parameters for WebSphere Code Release. The parameter should be provided without the Archive Install Option (for example, the parameter Archive Install Option Precompile JavaServer Pages is provided in the file as Precompile JavaServer Pages files).
		• Provide the key and value as supported by

Parameters Defined in this Step: Gather Advanced Parameters for WebSphere - Code Release , continued

Parameter Name	Example Value	Description
		IBM WebSphere. For example, `-contextroot /stock`

Parameters for WebSphere - Code Release

The following tables describe the required and optional input parameters for this workflow. For most parameters, if you do not specify a value for a parameter, a default value is assigned.

Parameters Defined in this Step: Gather Parameters for WebSphere - Code Release

Parameter Name	Default Value	Required	Description
Application Archive File List	no default	required	Comma-separated list of the Application Archive files to be deployed. Example: xxx.war or yyy.ear
Code Release History Location	no default	required	Fully qualified path name of the location where the application archive will be saved (for history purposes) on the target machine. This location cannot be the same as the Code Release Staging Location.
Code Release Staging Location	no default	required	Fully qualified path name of the location where the application archive will be saved on the target machine. This location cannot be the same as the Code Release History Location.
Enable Security	no default	required	Indicates whether security will be enabled. Valid values are True or False. If True then WebSphere Admin Password and WebSphere Admin User must have values.
MD5 Checksum	no default	required	Comma-separated list of the MD5 Checksum of the Application Archive files to be deployed.
Test URLs	no default	required	Comma-separated list of URLs used to test whether or not the list of applications deployed successfully. Example: http://mytestdb.com, http://yourtest.com

Parameters Defined in this Step: Gather Advanced Parameters for WebSphere - Code Release

Parameter Name	Default Value	Required	Description
Archive Install Option Allow Dispatching Includes to Remote	no default	optional	Specifies whether or not an application can dispatch includes to resources across web modules in different Java virtual machines in a

Parameters Defined in this Step: Gather Advanced Parameters for WebSphere - Code Release , continued

Parameter Name	Default Value	Required	Description
Resources			managed node environment through the standard request dispatcher mechanism. Possible values are Yes or No.
Archive Install Option Allow Servicing Includes from Remote Resources	no default	optional	Specifies whether or not an enterprise application can service an include request from an application. Possible values are Yes or No.
Archive Install Option Application Build ID	no default	optional	Specifies an uneditable string that identifies the Build ID version of the application.
Archive Install Option Asynchronous Request Dispatch Type	no default	optional	Specifies whether or not web modules can dispatch requests concurrently on separate threads, and if so, whether the server or client dispatches the requests. Concurrent dispatching can improve servlet response time.
Archive Install Option Business Level Application Name	no default	optional	Specifies that either the product creates a new business-level application name with the enterprise application that you are installing, or, makes the enterprise application a composition unit of an existing business-level application.
Archive Install Option Create MBeans for Resources	no default	optional	Specifies whether or not to create MBeans for resources such as servlets or JSP files within an application when the application starts. The default behavior is to create MBeans. Possible values are Yes or No.
Archive Install Option Deploy Enterprise Beans	no default	optional	Specifies whether or not the EJBDeploy tool runs during application installation. Possible values are Yes or No.
Archive Install Option Distribute Application	no default	optional	Specifies whether or not the product expands application binaries in the installation location during installation and deletes application binaries during uninstallation. The default is to enable application distribution. Application binaries for installed applications are expanded to the directory specified. Possible values are Yes or No.
Archive Install Option File Permission	no default	optional	Specifies access permissions for application binaries for installed applications that are expanded to the directory specified. Possible values are .*=755 or .*\.dll=755#.*\.so=755#.*\.a=755#.*\.sl=755 or

Parameters Defined in this Step: Gather Advanced Parameters for WebSphere - Code Release , continued

Parameter Name	Default Value	Required	Description
			.*\.htm=755#.*\.html=755#.*\.gif=755#.*\.jpg=755
Archive Install Option Override Class Reloading Settings for Web and EJB Modules	no default	optional	Specifies whether or not the product run time detects changes to application classes when the application is running. If enabled, and application classes are changed, then the application is stopped and restarted to reload updated classes. Possible values are Yes or No.
Archive Install Option Precompile JavaServer Pages Files	no default	optional	Specifies whether or not to precompile JavaServer Pages (JSP) files as a part of installation. The default is not to precompile JSP files. Possible values are Yes or No.
Archive Install Option Process Embedded Configuration	no default	optional	Specifies whether or not the embedded configuration should be processed. An embedded configuration consists of files such as resource.xml, variables.xml, and deployment.xml. You can collect WebSphere Application Server-specific deployment information and store it in the application EAR file. You can then install the EAR file into a WebSphere Application Server configuration using application management interfaces. Possible values are Yes or No.
Archive Install Option Reload Interval in Seconds	no default	optional	Specifies the number of seconds to scan the application's file system for updated files. The default is the value of the reloading interval attribute in the IBM extension (META-INF/ibm-application-ext.xmi) file of the EAR file. The reloading interval attribute takes effect only if class reloading is enabled. To enable reloading, specify a value greater than zero (for example, 1 to 2147483647). To disable reloading, specify zero (0). The range is from 0 to 2147483647.
Archive Install Option Use Binary Configuration	no default	optional	Specifies whether or not the application server uses the binding, extensions, and deployment descriptors located with the application deployment document, the deployment.xml file (default), or those located in the enterprise archive (EAR) file. Select this setting for applications installed on Version 6.0 or later deployment targets only. Possible values are Yes or No.

Parameters Defined in this Step: Gather Advanced Parameters for WebSphere - Code Release , continued

Parameter Name	Default Value	Required	Description
Archive Install Option Validate Install	no default	optional	Specifies whether or not the product examines the application references specified during application installation or updating and, if validation is enabled, warns users about incorrect references or fails the operation. Valid values are Off, Warn and Fail. Specify Off for no resource validation, Warn for warning messages about incorrect resource references, or Fail to stop operations that fail as a result of incorrect resource references.
Archive Settings File	no default	optional	The file containing the install options for all the archive files.
Cleanup on Failure	True	optional	Determines whether or not to remove downloaded and extracted files. This parameter also cleans up the installed directory upon failure of the workflow.
Cleanup on Success	True	optional	Determines whether or not to remove downloaded and extracted files. This parameter also cleans up the installed directory upon successful execution of the workflow.
JVM Generic Arguments	no default	optional	Specifies the JVM generic arguments. Provide values as standard JVM settings.
JVM System Properties	no default	optional	Specifies the JVM System Properties. Provide the string in the following format: 'PropertyName, PropertyValue||PropertyName, PropertyValue'
Web Service Password	no default	required	Password for the Web Service API.
Web Service URL	dma.url	required	URL for the HPE DMA Discovery web service API. Example: https://example.com/8443/dma
Web Service User	dma.user	required	A user capable of modifying the HPE DMA managed environment by using the web service API.
WebSphere Admin Password	no default	optional	The password for a user in a group that can change the state of a given application server. Only required if global security is enabled. It cannot not begin with a dash (-) or contain a space ( ).
WebSphere Admin Username	no default	optional	The user account for a user in a group that can

Parameters Defined in this Step: Gather Advanced Parameters for WebSphere - Code Release , continued

Parameter Name	Default Value	Required	Description
			change the state of a given application server. Only required if global security is enabled. It cannot begin with a dash (-), a period (.), or a space ( ). It cannot contain any of the following characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }.

WebSphere - Code Release on Cluster

This workflow automates the deployment of applications in IBM WebSphere. In addition to deployment, this workflow can update the JVM Generic Arguments and JVM System Properties on the Web Server, and also provides install options for the deployment of applications.

Some of the install options are provided as parameters to the workflow, or users can specify install options within a file for each of the applications to be deployed. Note, though, that the value provided for parameters takes higher precedence. This workflow supports the verification of the application deployments by providing the URLs.

For successful application deployments, verifications and a list of the applications are maintained in the History file. In cases of unsuccessful application deployments, the workflow rolls back the deployment and restores the last successfully deployed application (if any).

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

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

Prerequisites for this Workflow

Be sure that the following prerequisites are satisfied before you run the WebSphere - Code Release on Cluster workflow.

Product Platform

This workflow automates application deployments in IBM WebSphere 8 or WebSphere 8.5.x.

Dependencies

This workflow has the following dependencies:

- A working WebSphere Network Deployment cell, whose Deployment Manager is available for communication
- You must run the Discover WebSphere workflow before running this workflow. The Discover WebSphere workflow audits the server's physical environment for WebSphere cells, clusters, and application servers and then stores the configuration information in the HPE DMA environment.

For more information about prerequisites for WebSphere, refer to the WebSphere 8 Product Documentation.

How this Workflow Works

The following information describes how the WebSphere - Code Release On Cluster workflow works:

Overview

This workflow does the following things in the order shown:

1. Initially, the workflow inputs all parameters, set defaults for optional parameters, validates all parameters, and determines all members of the cluster. If input files do not exist in the specified locations, they are downloaded from the software repository. The workflow performs a checksum to verify that the archive files should be deployed in the Application Server on a cluster setup.
2. Next, the workflow creates the installation options and the call wrapper that will be used to execute commands within a WebSphere environment. The workflow updates the JVM setting and then creates a backup. The workflow deploys the specified Application Archive files in the Application Server on a cluster setup.
3. If the application deployment succeeds, the workflow tests the URLs for the web servers and copies the application archives.
4. If the application deployment fails, the workflow rolls back the deployment and restores the last successfully deployed application (if any).
5. Finally, the workflow cleans up downloaded files based on the Cleanup on Success and Cleanup on Failure parameters.

Validation Checks Performed

The workflow performs the following checks on the input parameters:

Enable Security	Must be true or false
If Enable Security is true	WebSphere Admin Username must be specified WebSphere Admin Password must be specified
WebSphere Admin Username	Cannot contain the following characters / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { } and also cannot begin with a dash (-), period (.), or space ( )
WebSphere Admin Password	Cannot begin with a dash (-) and cannot contain a space ( )
Code Release Staging Location Code Release History Location	Must be valid absolute paths Cannot have the same values
Application Archive File List Md5 Checksum	There must be a checksum for each Application Archive file The Application Archive files must be type `.ear` or `.war` and have valid absolute paths Checksums must be valid hexadecimal numbers

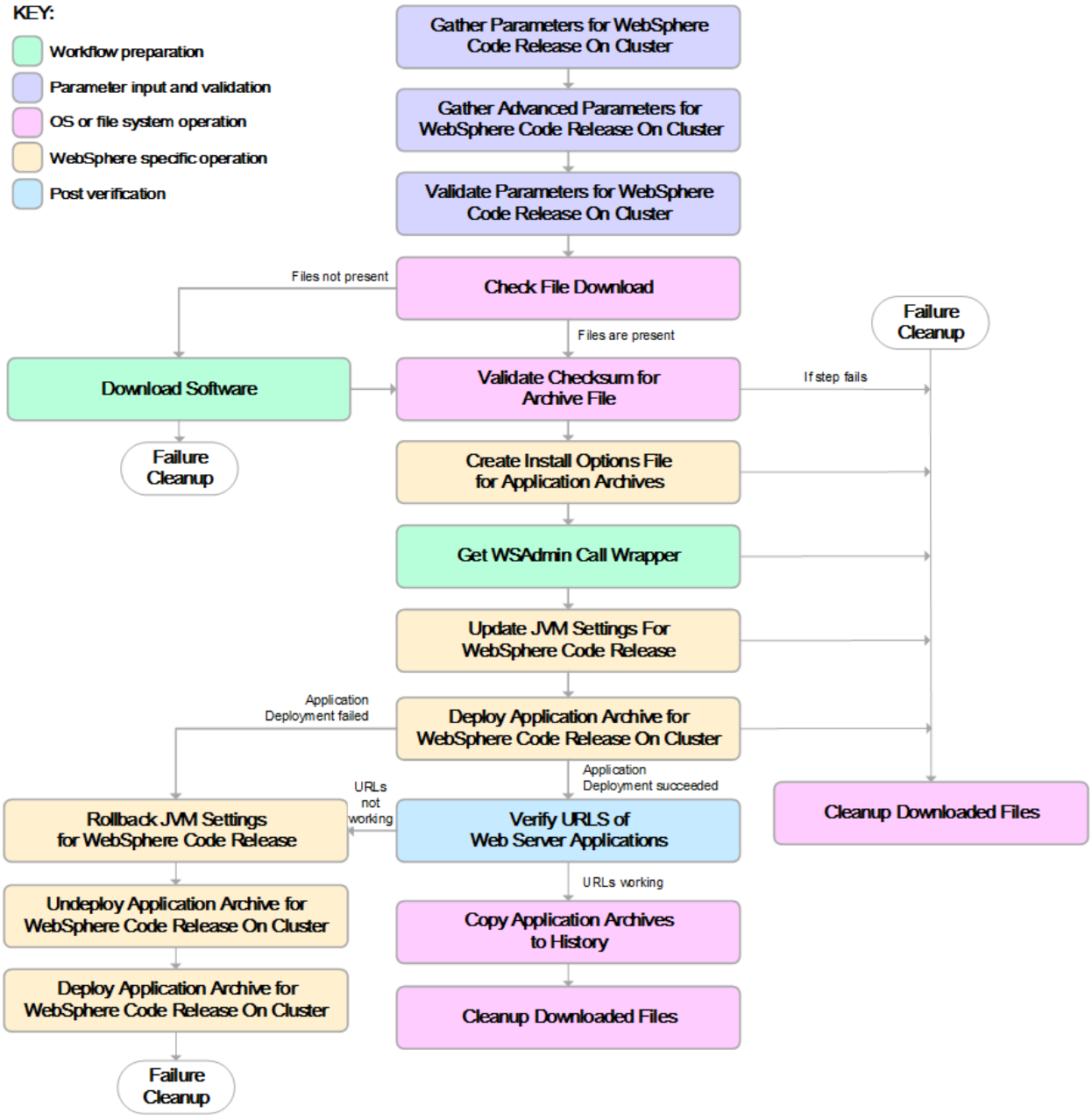
The WebSphere - Code Release On Cluster workflow also checks the environment for the following:

- The WebSphere container type must be cluster.
- The WebSphere Home exists.

Steps Executed

The workflow includes the following steps. Each step must complete successfully before the next step can start. If a step fails, the workflow reports a failure and subsequent steps are skipped, except for the Cleanup Downloaded Files step.

Click each box in the diagram to view additional information about that step.



Steps Used in the WebSphere - Code Release Workflow

Workflow Step	Description
Gather Parameters for WebSphere Code Release On Cluster	This step gathers mandatory input parameters (user-provided) used to deploy a list of application archives in a IBM WebSphere Application Server on a cluster setup.
Gather Advanced Parameters for WebSphere Code Release On Cluster	This step gathers the advanced input parameters (user-provided) used to deploy an application archive for a WebSphere Application Server on a cluster setup. Input parameters specified in this step are optional. Appropriate default values are specified.
Validate Parameters for WebSphere Code Release On Cluster	This step validates the basic and advanced parameters provided by the user, and checks the prerequisites for deploying a list of application archives for an IBM WebSphere Application Server on a cluster setup.
Check File Download	This step checks for the existence of a file before downloading from the HP Server Automation software repository. • Checks if file is in the expected location. • If the file is not in the expected location, generates a list of files for file download.
Download Software	This step downloads a list of files to a specified location on the target server.
Validate Checksum for Archive File	This step verifies the checksum for the archive files and archive setting file (if any) to ensure that the file has not changed and that the correct archives are deployed in the Application Server.
Create Install Options File for Application Archives	This step creates a setting file that includes the install options for the list of application archive files being deployed by the application server.
Get WSAdmin Call Wrapper	This step creates the necessary call wrapper to call `wsadmin` to execute certain operations within a given WebSphere environment.
Update JVM Settings For WebSphere Code Release	This step updates the JVM setting of the IBM WebSphere Application server. It also performs a backup of the IBM WebSphere profile configuration.
Deploy Application Archive for WebSphere Code Release On Cluster	Using the user-provided Application Archive files: This step deploys the list of application archives in the IBM WebSphere Application Server on a cluster

Steps Used in the WebSphere - Code Release Workflow, continued

Workflow Step	Description
	setup.
If the application deployment succeeds, the following steps are executed	
Verify URLS of Web Server Applications	This step verifies that the URLs are working, and looks for return status code values of 200 for success.
Copy Application Archives to History	This step copies the list of files from the staging location to the history location.
Cleanup Downloaded Files	For workflow success—and if Cleanup on Success is set to True (default)—this step removes all downloaded files and archives. Dependencies: Run as file/directory owner.
If the application deployment fails, the following steps are executed	
Rollback JVM Settings for WebSphere Code Release	This step restores a backup of the IBM WebSphere profile configuration.
Undeploy Application Archive for WebSphere Code Release On Cluster	This step uninstalls the list of application archives from a IBM WebSphere Application Server on a cluster setup.
Deploy Application Archive for WebSphere Code Release	Using the backup of the Application Archive files: This step deploys the list of application archives in the IBM WebSphere Application Server on a cluster setup.
Cleanup Downloaded Files	For workflow failure—and if Cleanup on Failure is set to True (default)—this step removes all downloaded files and archives. Dependencies: Run as file/directory owner.

For parameter descriptions and defaults, see "Parameters for WebSphere - Code Release on Cluster" on page 284.

How to Run this Workflow

The following instructions show you how to customize and run the WebSphere - Code Release on Cluster workflow in your environment.

The workflow provides default values for some parameters. These default values are usually sufficient for a "typical" installation. You can override the defaults by specifying parameter values in the deployment.

Note: Before following this procedure, review the Prerequisites for this Workflow, and ensure that all requirements are satisfied.

To use the WebSphere - Code Release on Cluster workflow:

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

   Parameters Defined in this Step: Gather Parameters for WebSphere - Code Release

Parameter Name	Default Value	Required	Description
Application Archive File List	no default	required	Comma-separated list of the Application Archive files to be deployed. Example: xxx.war or yyy.ear
Code Release History Location	no default	required	Fully qualified path name of the location where the application archive will be saved (for history purposes) on the target machine. This location cannot be the same as the Code Release Staging Location.
Code Release Staging Location	no default	required	Fully qualified path name of the location where the application archive will be saved on the target machine. This location cannot be the same as the Code Release History Location.
Enable Security	no default	required	Indicates whether security will be enabled. Valid values are True or False. If True then WebSphere Admin Password and WebSphere Admin User must have values.
MD5 Checksum	no default	required	Comma-separated list of the MD5 Checksum of the Application Archive files to be deployed.
Test URLs	no default	required	Comma-separated list of URLs used to test whether or not the list of applications deployed successfully. Example: http://mytestdb.com, http://yourtest.com

   Tip: To avoid having to re-enter passwords whenever they change, you can create a policy to provide them to the workflow.

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

   See "Parameters for WebSphere - Code Release on Cluster" on page 284 for detailed descriptions of all input parameters for this workflow, including default values.

3. In the workflow editor, expose any additional parameters that you need. You will specify values for those parameters when you create the deployment
4. Save the changes to the workflow (click **Save** in the lower right corner).
5. Create a new deployment.
6. On the Parameters tab, specify values for the required parameters listed in step 2 and any additional

parameters that you have exposed.You do not need to specify values for those parameters whose default values are appropriate for your environment.

7. On the Targets tab, specify one or more targets for this deployment.
8. Save the deployment (click **Save** in the lower right corner).
9. Run the workflow using this deployment.

To verify the results:

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

Optional: If you want to further verify the results:

Use the WebSphere administrative console interface to check that the web server is configured.

Sample Scenario

This topic shows you typical parameter values for different use cases for the WebSphere - Code Release on Cluster workflow. For a complete list of all parameters used in this workflow, including default values, see "Parameters for WebSphere - Code Release on Cluster" on page 284.

Tip: To avoid having to re-enter passwords whenever they change, you can create a policy to provide them to the workflow.

Scenario 1: Install an application archive (for example stocksanalysis.war) on a running IBM WebSphere Application Server on a standalone setup.

In this scenario we will deploy the stockanalysis.war file on a running IBM WebSphere Application Server. We will install the application using the default installation options. If the application archive files are not present in the Code Release Staging Location, then they will be downloaded from the SA Repository.

Parameters Defined in this Step: Gather Parameters for WebSphere - Code Release

Parameter Name	Default Value	Description
Application Archive File List	stockanalysis.war	Comma-separated list of the Application Archive files to be deployed. Example: xxx.war or yyy.ear
Code Release History Location	/opt/IBM/was/history	Fully qualified path name of the location where the application archive will be saved (for history purposes) on the target machine. This location cannot be the same as the Code Release Staging Location.
Code Release Staging Location	/tmp/IBM/was/staging	Fully qualified path name of the location where the application archive will be saved on the target machine. This location cannot be the same as the Code Release History Location.

Parameters Defined in this Step: Gather Parameters for WebSphere - Code Release , continued

Parameter Name	Default Value	Description
Enable Security	False	Indicates whether security will be enabled. Valid values are True or False. If True then WebSphere Admin Password and WebSphere Admin User must have values.
MD5 Checksum	4477e994e9d457ad2214a3d36b1bb16b	Comma-separated list of the MD5 Checksum of the Application Archive files to be deployed.
Test URLs	http://<server:port>/stockanalysis/<xyx.html>	Comma-separated list of URLs used to test whether or not the list of applications deployed successfully. Example: http://mytestdb.com, http://yourtest.com

Scenario 2: Install an application archive (for example stocksanalysis.war) on a running IBM WebSphere Application Server on a standalone setup.

In this scenario we will deploy the stockanalysis.war file on a running IBM WebSphere Application Server. We will install the application using the default installation options. The JVM settings are also applied to the Application server. If the application archive files are not present in the Code Release Staging Location, then they will be downloaded from the SA Repository.

Parameters Defined in this Step: Gather Parameters for WebSphere - Code Release

Parameter Name	Default Value	Description
Application Archive File List	stockanalysis.war	Comma-separated list of the Application Archive files to be deployed. Example: xxx.war or yyy.ear
Code Release History Location	/opt/IBM/was/history	Fully qualified path name of the location where the application archive will be saved (for history purposes) on the target machine. This location cannot be the same as the Code Release Staging Location.
Code Release Staging Location	/tmp/IBM/was/staging	Fully qualified path name of the location where the application archive will be saved on the target machine. This location cannot be the same as the Code Release History Location.
Enable Security	False	Indicates whether security will be enabled. Valid values are True or False. If True then WebSphere Admin

Parameters Defined in this Step: Gather Parameters for WebSphere - Code Release , continued

Parameter Name	Default Value	Description
		Password and WebSphere Admin User must have values.
MD5 Checksum	4477e994e9d457ad2214a3d36b1bb16b	Comma-separated list of the MD5 Checksum of the Application Archive files to be deployed.
Test URLs	http://<server:port>/stockanalysis/<xyx.html>	Comma-separated list of URLs used to test whether or not the list of applications deployed successfully. Example: http://mytestdb.com, http://yourtest.com

Parameters Defined in this Step: Gather Advanced Parameters for WebSphere - Code Release

Parameter Name	Default Value	Description
JVM Generic Arguments	• Dclient.encoding.override=UTF-8 • Dsun.rmi.dgc.client.gcInterval=3600000000 • Dsun.rmi.dgc.server.gcInterval=3600000000	Specifies the JVM generic arguments. Provide values as standard JVM settings.
JVM System Properties	stockanalysis _home, /opt/stockanalysis/bin, Home path for the stock analysis	Specifies the JVM System Properties. Provide the string in the following format: 'PropertyName, PropertyValue||PropertyName, PropertyValue'

Scenario 3: Install an application archive (for example stocksanalysis.war) on a running IBM WebSphere Application Server on a standalone setup.

In this scenario we deploy the stockanalysis.war file on a running IBM WebSphere Application Server. We will install the application using the default installation options. This scenario provides the install options to deploy the application archive in a file. If the Application Archive Files and the Archive Setting File are not present in the Code Release Staging Location, then they will be downloaded from the SA Repository.

Parameters Defined in this Step: Gather Parameters for WebSphere - Code Release

Parameter Name	Default Value	Description
Application Archive File List	stockanalysis.war	Comma-separated list of the Application Archive files to be deployed. Example: xxx.war or yyy.ear
Code Release History Location	/opt/IBM/was/history	Fully qualified path name of the location where the application archive will be saved (for history purposes) on the target machine. This location

Parameters Defined in this Step: Gather Parameters for WebSphere - Code Release , continued

Parameter Name	Default Value	Description
		cannot be the same as the Code Release Staging Location.
Code Release Staging Location	/tmp/IBM/was/staging	Fully qualified path name of the location where the application archive will be saved on the target machine. This location cannot be the same as the Code Release History Location.
Enable Security	False	Indicates whether security will be enabled. Valid values are True or False. If True then WebSphere Admin Password and WebSphere Admin User must have values.
MD5 Checksum	4477e994e9d457ad2214a3d36b1bb16, 1eff908bedaa416c104f6b4a9a268233	Comma-separated list of the MD5 Checksum of the Application Archive files to be deployed.
Test URLs	http://<server:port>/*stock*/<xyx.html>	Comma-separated list of URLs used to test whether or not the list of applications deployed successfully. Example: http://mytestdb.com, http://yourtest.com

Parameters Defined in this Step: Gather Advanced Parameters for WebSphere - Code Release

Parameter Name	Default Value	Description

Archive Settings File	archive.setting	The file containing the install options for all the archive files.
		Sample Archive Settings File content:
		`stockanalysis.war = {`
		`Precompile JavaServer Pages files = No`
		`-contextroot /stock`
		`}`
		Options for providing the key are:
		• Provide the key in plain English. The key supported is the parameter name in the step Gather Advanced Parameters for WebSphere Code Release. The parameter should be provided without the Archive Install Option (for example, the parameter Archive Install Option Precompile JavaServer Pages is provided in the file as Precompile JavaServer Pages files).
		• Provide the key and value as supported by IBM

Parameters Defined in this Step: Gather Advanced Parameters for WebSphere - Code Release , continued

Parameter Name	Default Value	Description
		WebSphere. For example, `-contextroot /stock`

Parameters for WebSphere - Code Release on Cluster

The following tables describe the required and optional input parameters for this workflow.For most parameters, if you do not specify a value for a parameter, a default value is assigned.

Parameters Defined in this Step: Gather Parameters for WebSphere - Code Release on Cluster

Parameter Name	Default Value	Required	Description
Application Archive File List	no default	required	Comma-separated list of the Application Archive files to be deployed. Example: xxx.war or yyy.ear
Code Release History Location	no default	required	Fully qualified path name of the location where the application archive will be saved (for history purposes) on the target machine. This location cannot be the same as the Code Release Staging Location.
Code Release Staging Location	no default	required	Fully qualified path name of the location where the application archive will be saved on the target machine. This location cannot be the same as the Code Release History Location.
Enable Security	no default	required	Indicates whether security will be enabled. Valid values are True or False. If True then WebSphere Admin Password and WebSphere Admin User must have values.
MD5 Checksum	no default	required	Comma-separated list of the MD5 Checksum of the Application Archive files to be deployed.
Test URLs	no default	required	Comma-separated list of URLs used to test whether or not the list of applications deployed successfully. Example: http://mytestdb.com, http://yourtest.com

Parameters Defined in this Step: Gather Advanced Parameters for WebSphere - Code Release on Cluster

Parameter Name	Default Value	Required	Description
Archive Install Option Allow Dispatching Includes to Remote Resources	no default	optional	Specifies whether or not an application can dispatch includes to resources across web modules in different Java virtual machines in a managed node environment through the standard request dispatcher mechanism. Possible values are Yes or No.
Archive Install Option Allow Servicing Includes from Remote Resources	no default	optional	Specifies whether or not an enterprise application can service an include request from an application. Possible values are Yes or No.
Archive Install Option Application Build ID	no default	optional	Specifies an uneditable string that identifies the Build ID version of the application.
Archive Install Option Asynchronous Request Dispatch Type	no default	optional	Specifies whether or not web modules can dispatch requests concurrently on separate threads, and if so, whether the server or client dispatches the requests. Concurrent dispatching can improve servlet response time.
Archive Install Option Business Level Application Name	no default	optional	Specifies that either the product creates a new business-level application name with the enterprise application that you are installing, or, makes the enterprise application a composition unit of an existing business-level application.
Archive Install Option Create MBeans for Resources	no default	optional	Specifies whether or not to create MBeans for resources such as servlets or JSP files within an application when the application starts. The default behavior is to create MBeans. Possible values are Yes or No.
Archive Install Option Deploy Enterprise Beans	no default	optional	Specifies whether or not the EJBDeploy tool runs during application installation. Possible values are Yes or No.
Archive Install Option Distribute Application	no default	optional	Specifies whether or not the product expands application binaries in the installation location during installation and deletes application binaries during uninstallation. The default is to enable application distribution. Application binaries for installed applications are expanded to the directory specified. Possible values are Yes or No.

Parameters Defined in this Step: Gather Advanced Parameters for WebSphere - Code Release on Cluster, continued

Parameter Name	Default Value	Required	Description
Archive Install Option File Permission	no default	optional	Specifies access permissions for application binaries for installed applications that are expanded to the directory specified. Possible values are .*=755 or .*\.dll=755#.*\.so=755#.*\.a=755#.*\.sl=755 or .*\.htm=755#.*\.html=755#.*\.gif=755#.*\.jpg=755
Archive Install Option Override Class Reloading Settings for Web and EJB Modules	no default	optional	Specifies whether or not the product run time detects changes to application classes when the application is running. If enabled, and application classes are changed, then the application is stopped and restarted to reload updated classes. Possible values are Yes or No.
Archive Install Option Precompile JavaServer Pages Files	no default	optional	Specifies whether or not to precompile JavaServer Pages (JSP) files as a part of installation. The default is not to precompile JSP files. Possible values are Yes or No.
Archive Install Option Process Embedded Configuration	no default	optional	Specifies whether or not the embedded configuration should be processed. An embedded configuration consists of files such as resource.xml, variables.xml, and deployment.xml. You can collect WebSphere Application Server-specific deployment information and store it in the application EAR file. You can then install the EAR file into a WebSphere Application Server configuration using application management interfaces. Possible values are Yes or No.
Archive Install Option Reload Interval in Seconds	no default	optional	Specifies the number of seconds to scan the application's file system for updated files. The default is the value of the reloading interval attribute in the IBM extension (META-INF/ibm-application-ext.xmi) file of the EAR file. The reloading interval attribute takes effect only if class reloading is enabled. To enable reloading, specify a value greater than zero (for example, 1 to 2147483647). To disable reloading, specify zero (0). The range is from 0 to 2147483647.
Archive Install Option Use Binary Configuration	no default	optional	Specifies whether or not the application server uses the binding, extensions, and deployment descriptors located with the application deployment document, the deployment.xml file (default), or those located in the enterprise archive (EAR) file. Select this setting for applications installed on Version 6.0 or later deployment targets only. Possible values are Yes or No.
Archive Install Option Validate	no default	optional	Specifies whether or not the product examines the application references specified during application installation or updating

Parameters Defined in this Step: Gather Advanced Parameters for WebSphere - Code Release on Cluster, continued

Parameter Name	Default Value	Required	Description
Install			and, if validation is enabled, warns users about incorrect references or fails the operation. Valid values are Off, Warn and Fail. Specify Off for no resource validation, Warn for warning messages about incorrect resource references, or Fail to stop operations that fail as a result of incorrect resource references.
Archive Settings File	no default	optional	The file containing the install options for all the archive files.
Cleanup on Failure	True	optional	Determines whether or not to remove downloaded and extracted files. This parameter also cleans up the installed directory upon failure of the workflow.
Cleanup on Success	True	optional	Determines whether or not to remove downloaded and extracted files. This parameter also cleans up the installed directory upon successful execution of the workflow.
JVM Generic Arguments	no default	optional	Specifies the JVM generic arguments. Provide values as standard JVM settings.
JVM System Properties	no default	optional	Specifies the JVM System Properties. Provide the string in the following format: 'PropertyName, PropertyValue||PropertyName, PropertyValue'
Web Service Password	no default	required	Password for the Web Service API.
Web Service URL	dma.url	required	URL for the HPE DMA Discovery web service API. Example: https://example.com/8443/dma
Web Service User	dma.user	required	A user capable of modifying the HPE DMA managed environment by using the web service API.
WebSphere Admin Password	no default	optional	The password for a user in a group that can change the state of a given application server. Only required if global security is enabled. It cannot not begin with a 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 / \ * , : ; = + ? | < > & % ' " [ ] # $ ^ { }.

WebSpehere 8 - Patch Network Cell

The workflow supports the patching of WebSphere 8.0 or 8.5.x running in a Network Deployment topology and standalone profile. This workflow patches WebSphere 8 instances which are installed by root as well as non-root users. For non-root user installation, patching step of the workflow will run as the user account that has installed WebSphere 8.

Fixes and updates are installed by the workflow using an existing instance of the IBM Installation Manager software, which must exist on each target machine.

This workflow takes into account the multiple components related to a Network Deployment implementation and makes sure that all components (`dmgr`, `nodeagent`, and application servers) are stopped before proceeding with the patching.

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

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

Prerequisites for this Workflow

Be sure that the following prerequisites are satisfied before you run this workflow:

1. You have installed the HPE DMA Database Release Management solution pack.
2. You have a valid HP Software support contract for this solution pack.
3. You have downloaded and installed all available HPE DMA patches and hot fixes.
4. IBM Installation Manager software exists on each target machine.

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

https://softwaresupport.hp.com/

Dependencies:

- This workflow runs as root. However, it will patch a non-root WebSphere 8.0 or 8.5.x Installation. The workflow runs the patch step as the user that installed WebSphere 8.0 or 8.5.x (installed user).
- The workflow supports the patching of WebSphere 8.0 or 8.5.x running in a Network Deployment topology and standalone profile.
- When patching a Network Deployment Cell, the workflow must be set up to first patch the server that runs the Deployment Manager process and then patch the other nodes in the cell.
- The workflow requires that an instance of IBM Installation Manager be installed on each of the target servers.

For information about prerequisites for WebSphere 8.0 or 8.5.x, refer to the WebSphere 8 Product Documentation.

How this Workflow Works

The following information describes how the "WebSpehere 8 - Patch Network Cell" workflow works:

Overview show

This workflow installs cumulative fixes and updates for a WebSphere 8.0 or 8.5.x application server.

The workflow supports the patching of WebSphere 8.0 or 8.5.x running in a Network Deployment topology and standalone profile.

Validation Checks Performed show

The validation centers on the input parameters:

- The input parameters have the proper syntax (no special characters or spaces).
- Specified files exist and have valid permissions.

Steps Executed show

The WebSpehere 8 - Patch Network Cell workflow includes the following steps. Each step must complete successfully before the next step can start. If a step fails, the workflow restores the configuration, cleans up files as necessary, reports a failure, and skips all subsequent steps.

Steps for WebSpehere 8 - Patch Network Cell

Workflow Step	Description
Gather Parameters For WebSphere8 Network Cell Patching	Gathers the required parameters needed to patch the IBM WebSphere Application Server V8.0 and 8.5.x.
Gather Advanced Parameters For WebSphere8 Network Cell Patching	Gathers the optional parameters needed to patch the IBM WebSphere Application Server V8.0 and 8.5.x.
Get WSAdmin Call Wrapper	Creates the necessary call wrapper to call `wsadmin` to execute certain operations within the WebSphere 8.0 or 8.5.x environment.
Validate Parameters For WebSphere8 Patching Network Cell	This step validates the basic and advanced parameters provided by the user, and checks the prerequisites for patching the IBM WebSphere Application Server.
Check File Download	Checks for the existence of a file on the target machine before downloading that file from the HPE DMA server. For each file in the list: 1. The step determines whether the file is in the expected location on the target machine. 2. If the file is not in the expected location, the step adds that file to a list of files that need to be downloaded.
Download Software	Automates the transfer of files from the software repository to individual managed servers for use in downstream workflow steps.
WebSphere Backup Config	Uses the `backupConfig` utility to backup the WebSphere configurations for the specified WebSphere 8.0 or 8.5.x installation.
Verify Install Manager Exists	Verifies that an IBM Installation Manager instance exists on each of the specified target machines.
WebSphere Patching Extract Archive v2	First checks to ensure that the archive file exists. Then, based on the archive extension, extracts the archive to the specified directory.
WebSphere Stop Application Servers v2	Stops all application servers that are in started state before patching the installation of WebSphere.
WebSphere Stop Management Processes v2	First stops `nodeagents`. If there is a `dmgr` process running, the step will then stop that process before patching the WebSphere 8.0 or 8.5.x installation.
Verify All Java Processes Stopped	Verifies that all Java processes relevant to the WebSphere services on the specified target have been stopped.

Steps for WebSpehere 8 - Patch Network Cell, continued

Workflow Step	Description
WebSphere Apply Patches v2	Uses the IBM Installation Manager to apply the cumulative patches to the specified WebSphere 8.0 or 8.5.x installation.
WebSphere Start Management Processes v2	First starts the `dmgr` process first if one exists. Then, starts the `nodeagent` process.
WebSphere Restore Config	If the patching process fails, this step is called to restore the configuration via the `restoreConfig` utility.
WebSphere Start Application Servers v2	Starts only the application servers that were stopped by the WebSphere Stop Application Servers step.
WebSphere Start Management Processes	First starts the `dmgr` process first if one exists. Then, starts the `nodeagent` process.
WebSphere Cleanup Downloaded Files	Removes all temporary downloaded files and archives.
WebSphere Start Application Servers v2	Starts only the application servers that were stopped by the WebSphere Stop Application Servers step.
Discover WebSphere	Examines the target server's physical environment to discover information about WebSphere 8 cells, clusters, and managed servers. **Note:** Discovery is ONLY additive. It will not remove instances or databases currently in your environment. It is your HPE DMA administrator's responsibility to delete content that is no longer in use.

For parameter descriptions and defaults, see "Parameters for WebSpehere 8 - Patch Network Cell".

How to Run this Workflow

The following instructions show you how to customize and run the "WebSpehere 8 - Patch Network Cell" workflow in your environment.

Note: Before following this procedure, review the "Prerequisites for this Workflow" on page 289, and ensure that all requirements are satisfied.

To use the Patch WebSphere 8 Network Deployment Cell workflow:

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

Parameter Name	Default Value	Required	Description
Config Backup File	no default	required	Fully qualified file path where the WebSphere BackupConfig utility will write the backup file. For example: `/opt/IBM/WebSphere/newbackup/backup.zip`
Enable Security	true	required	Enables administrative security. Must be set to either true or false. If Enable Security is true, the WAS Admin User and WAS Admin Password parameters must have values.
WAS Admin Password	myPwd	required	If global security is enabled, this is the password for a user who belongs to a group that has permission to change the state of a specific application server.
WAS Admin User	myUsername	required	If global security is enabled, this is the user account for a user who belongs to a group that has permission to change the state of a specific application server.
WebSphere Install Location	see description	required	Fully qualified file path of the specific IBM WebSphere Application Server installation which needs to be patched. For example: `/usr/IBM/WebSphere/AppServer` or `/opt/IBM/WebSphere/AppServer`
WebSphere Patch File List	no default	required	Comma-separated list of WebSphere cumlative patch files on the target machine. For example: `8.0.0-WS-WAS-FP0000003-part1.zip, 8.0.0-WS-WAS-FP0000003-part2.zip`
WebSphere Staging Location	no default	required	Fully qualified file path of the location where the list of patch files are downloaded. `usr/IBM/patches/` or `tmp/IBM/patches/`

Tip: To avoid having to re-enter passwords whenever they change, you can create a policy to provide them to the workflow.

> **Note:** See "Parameters for WebSpehere 8 - Patch Network Cell" on page 297 for detailed descriptions of all input parameters for this workflow, including default values.

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

To verify the results:

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

Sample Scenario

It is very straightforward to run the "WebSpehere 8 - Patch Network Cell" workflow. This topic shows you typical parameter values to use.

For the sample use case scenario below, security is enabled.

Parameter Name	Example Value	Description
Config Backup File	no default	Fully qualified file path where the WebSphere BackupConfig utility will write the backup file. For example: `/opt/IBM/WebSphere/newbackup/backup.zip`
Enable Security	true	Enables administrative security. Must be set to either true or false. If Enable Security is true, the WAS Admin User and WAS Admin Password parameters must have values.
WAS Admin Password	myPwd	If global security is enabled, this is the password for a user who belongs to a group that has permission to change the state of a specific application server.
WAS Admin User	myUsername	If global security is enabled, this is the user account for a user who belongs to a group that has permission to change the state of a specific application server.
WebSphere Install Location	see description	Fully qualified file path of the specific IBM WebSphere Application Server installation which needs to be patched. For example: `/usr/IBM/WebSphere/AppServer` or `/opt/IBM/WebSphere/AppServer`
WebSphere Patch File List	no default	Comma-separated list of WebSphere cumlative patch files on the target machine. For example: `8.0.0-WS-WAS-FP0000003-part1.zip`, `8.0.0-WS-WAS-FP0000003-part2.zip`
WebSphere Staging Location	no default	Fully qualified file path of the location where the list of patch files are downloaded. `usr/IBM/patches/` or `tmp/IBM/patches/`

Parameters for WebSpehere 8 - Patch Network Cell

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

Parameters Defined in this Step: Gather Parameters For WebSphere8 Network Cell Patching

Parameter Name	Default Value	Required	Description
Config Backup File	no default	required	Fully qualified file path where the WebSphere BackupConfig utility will write the backup file. For example: `/opt/IBM/WebSphere/newbackup/backup.zip`
Enable Security	true	required	Enables administrative security. Must be set to either true or false. If Enable Security is true, the WAS Admin User and WAS Admin Password parameters must have values.
WAS Admin Password	myPwd	required	If global security is enabled, this is the password for a user who belongs to a group that has permission to change the state of a specific application server.
WAS Admin User	myUsername	required	If global security is enabled, this is the user account for a user who belongs to a group that has permission to change the state of a specific application server.
WebSphere Install Location	see description	required	Fully qualified file path of the specific IBM WebSphere Application Server installation which needs to be patched. For example: `/usr/IBM/WebSphere/AppServer` or `/opt/IBM/WebSphere/AppServer`
WebSphere Patch File List	no default	required	Comma-separated list of WebSphere cumlative patch files on the target machine. For example: `8.0.0-WS-WAS-FP0000003-part1.zip`, `8.0.0-WS-WAS-FP0000003-part2.zip`
WebSphere Staging Location	no default	required	Fully qualified file path of the location where the list of patch files are downloaded. `usr/IBM/patches/` or `tmp/IBM/patches/`

Send Documentation Feedback

If you have comments about this document, you can contact the documentation team by email. If an email client is configured on this system, click the link above and an email window opens with the following information in the subject line:

Feedback on Workflows for IBM WebSpehere (Database and Middleware Automation 10.40)

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to hpe_dma_docs@hpe.com.

We appreciate your feedback!