



# HP Database and Middleware Automation

Software Version: 10.30  
Linux and Solaris

## WebLogic Provisioning User Guide

Document Release Date: May 2015  
Software Release Date: May 2015

## Legal Notices

### Warranty

The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

The information contained herein is subject to change without notice.

### Restricted Rights Legend

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

### Copyright Notice

© Copyright 2012-2015 Hewlett-Packard Development Company, L.P.

### Trademark Notices

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

UNIX® is a registered trademark of The Open Group.

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

## Documentation Updates

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

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

To check for recent updates or to verify that you are using the most recent edition of a document, 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 **Register** link at the top of the HP Software Support page.

You will also receive updated or new editions if you subscribe to the appropriate product support service.

Contact your HP sales representative for details.

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

### Document Changes

Chapter	Version	Changes
<a href="#">Title Page</a> <a href="#">Legal Notices</a>	10.01	Updated version number, software release date, document release date, and copyright date range.
<a href="#">WebLogic Provisioning Quick Start</a>	10.01	Updated from 10.00 to 10.01.

## Document Changes, continued

Chapter	Version	Changes
<a href="#">Title Page</a> <a href="#">Legal Notices</a>	10.10	Updated version number, software release date, document release date, and copyright date range.
<a href="#">About HP DMA Solution Packs</a>	10.10	Added overview topic: About HP DMA Solution Packs.
<a href="#">Title Page</a> <a href="#">Legal Notices</a>	10.20	Updated version number, software release date, document release date, and copyright date range.
<a href="#">WebLogic Provisioning Quick Start</a> <a href="#">Workflow Details</a>	10.20	Removed Quick Start chapter. In the "How to Run this Workflow" topics, pointed to the <i>HP DMA Quick Start Tutorial</i> .
<a href="#">The WebLogic Provisioning Solution</a> <a href="#">Workflow Details</a>	10.20	Listed deprecated workflows. Updated the following workflows: <a href="#">WebLogic - Provision Weblogic Software</a> <a href="#">WebLogic - Provision Weblogic Domain and Admin Server</a> <a href="#">WebLogic - Provision Weblogic Managed Servers</a> Added the following workflows: <a href="#">WebLogic - Create Trust and Identity Keystore</a> <a href="#">WebLogic - Provision Advanced Domain and Admin Server</a>
<a href="#">Title Page</a> <a href="#">Legal Notices</a> Entire guide	10.21	Updated version number, software release date, document release date, and copyright date range. Updated document template.
<a href="#">Title Page</a> <a href="#">Legal Notices</a>	10.22	Updated version number, software release date, document release date, and copyright date range.
<a href="#">Title Page</a> <a href="#">Legal Notices</a> Entire guide	10.30	Updated version number, software release date, document release date, and copyright date range. Updated to new documentation template.

## Support

Visit the HP 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 HP Software offers.

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

- Search for knowledge documents of interest
- Submit and track support cases and enhancement requests
- Download software patches
- Manage support contracts
- Look up HP support contacts
- Review information about available services

- Enter into discussions with other software customers
- Research and register for software training

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

**<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 HPSW Solution and Integration Portal Web site. This site enables you to explore HP Product Solutions to meet your business needs, includes a full list of Integrations between HP 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>**

# Contents

About HP DMA Solution Packs .....	7
Audience .....	8
Document Map .....	9
Important Terms .....	10
Chapter 1: The WebLogic Provisioning Solution .....	11
What this Solution Includes .....	13
Deprecated WebLogic Provisioning Workflows .....	14
Supported Products and Platforms .....	15
Prerequisites .....	16
Chapter 2: Workflow Details .....	17
How to Use the Workflows Together .....	19
WebLogic - Create Trust and Identity Keystore .....	21
Prerequisites for this Workflow .....	22
How this Workflow Works .....	23
How to Run this Workflow .....	25
Sample Scenario .....	28
Parameters for WebLogic - Create Trust and Identity Keystore .....	30
WebLogic - Provision Weblogic Software .....	32
Prerequisites for this Workflow .....	34
How this Workflow Works .....	35
How to Run this Workflow .....	39
Sample Scenario .....	43
Parameters for WebLogic - Provision Weblogic Software .....	48
WebLogic - Provision Weblogic Domain and Admin Server .....	51
Prerequisites for this Workflow .....	53
How this Workflow Works .....	54
How to Run this Workflow .....	57
Sample Scenario .....	60
Parameters for WebLogic - Provision Weblogic Domain and Admin Server .....	64
WebLogic - Provision Advanced Domain and Admin Server .....	67
Prerequisites for this Workflow .....	68
How this Workflow Works .....	69
How to Run this Workflow .....	72
Sample Scenario .....	75
Parameters for WebLogic - Provision Advanced Domain and Admin Server .....	77
WebLogic - Provision Weblogic Managed Servers .....	79
Prerequisites for this Workflow .....	81

How this Workflow Works .....	82
How to Run this Workflow .....	85
Sample Scenario .....	90
Parameters for WebLogic - Provision Weblogic Managed Servers .....	96
Provision WebLogic Cluster .....	100
Prerequisites for this Workflow .....	102
How this Workflow Works .....	103
How to Run this Workflow .....	106
Sample Scenario .....	108
Parameters for Provision WebLogic Cluster .....	110
Increase WebLogic Domain Span .....	112
Prerequisites for this Workflow .....	114
How this Workflow Works .....	115
How to Run this Workflow .....	117
Sample Scenario .....	120
Parameters for Increase WebLogic Domain Span .....	122
<b>Chapter 3: Reference Information .....</b>	<b>125</b>
WebLogic Product Documentation .....	125
HP DMA Documentation .....	125
<b>Chapter 4: Tips and Best Practices .....</b>	<b>126</b>
How a Solution Pack is Organized .....	127
How to Expose Additional Workflow Parameters .....	131
How to Use a Policy to Specify Parameter Values .....	132
Create a Policy .....	132
Extract a Policy .....	133
Reference the Policy in the Deployment .....	134
How to Import a File into the Software Repository .....	135
<b>Chapter 5: Troubleshooting .....</b>	<b>136</b>
Target Type .....	136
User Permissions and Related Requirements .....	136
Discovery in HP DMA .....	137
<b>Glossary .....</b>	<b>138</b>

# About HP DMA Solution Packs

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

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

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

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

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

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

# Audience

This solution is designed for:

- IT architects and engineers who are responsible for planning, implementing, and maintaining application-serving environments using Oracle® WebLogic Server version 11g or 12c
- Engineers who are implementing—or planning to implement—HP Database and Middleware Automation (HP DMA)

To use this solution effectively, you should be familiar with WebLogic 11g or 12c and its requirements (see links to the [WebLogic Product Documentation](#) on page 125).

# Document Map

The following table shows you how to navigate this guide:

Topic	Description
<a href="#">The WebLogic Provisioning Solution</a>	General information about this solution, including what it contains and what it does.
<a href="#">Workflow Details</a>	Information about the WebLogic 11g and 12c workflows included in this solution, including: prerequisites, how it works, how to run it, sample scenarios, and a list of input parameters.
<a href="#">Reference Information</a>	Links to current WebLogic 11g and 12c product documentation and additional HP DMA documentation.
<a href="#">Tips and Best Practices</a>	Simple procedures that you can use to accomplish a variety of common HP DMA tasks.
<a href="#">Troubleshooting</a>	Tips for solving common problems.

# Important Terms

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

- In HP DMA, a **workflow** executes a process —such as installing a software product or checking a database instance for compliance with a specific security benchmark.
- A workflow consists of a sequence of **steps**. Each step performs a very specific task. Steps can be shared among workflows.

- Steps can have input and output **parameters**, whose values will be unique to your environment. If you provide correct values for the input parameters that each scenario requires, the workflow will be able to accomplish its objective. Output parameters from one step often serve as input parameters to another step.

- A **solution pack** contains a collection of related workflows and the steps, functions, and policies that implement each workflow.

More precisely, solution packs contain **workflow templates**. These are read-only versions of the workflows that cannot be deployed. To run a workflow included in a solution pack, you must first create a deployable copy of the workflow template and then customize that copy for your environment.

- A **deployment** associates a workflow with the targets (servers, instances, or databases) where the workflow will run. To run a workflow, you execute a specific deployment. A deployment is associated with one workflow; a workflow can have many deployments, each with its own targets and parameter settings.

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

Organizations also have role-based permissions. Servers, instances, and databases inherit their role-based permissions from the organization in which the server resides.

- The **software repository** contains any files that a workflow might need to carry out its purpose (for example, software binaries or patch archives). If the files that a workflow requires are not in the software repository, they must be stored locally on each target server.

When you are using HP DMA with HP Server Automation (HP SA), the software repository is the HP SA Software Library.

- An **organization** is a logical grouping of servers. You can use organizations to separate development, staging, and production resources—or to separate logical business units. Because user security for running workflows is defined at the organization level, organizations should be composed with user security in mind.

Additional terms are defined in the [Glossary](#) on page 138.

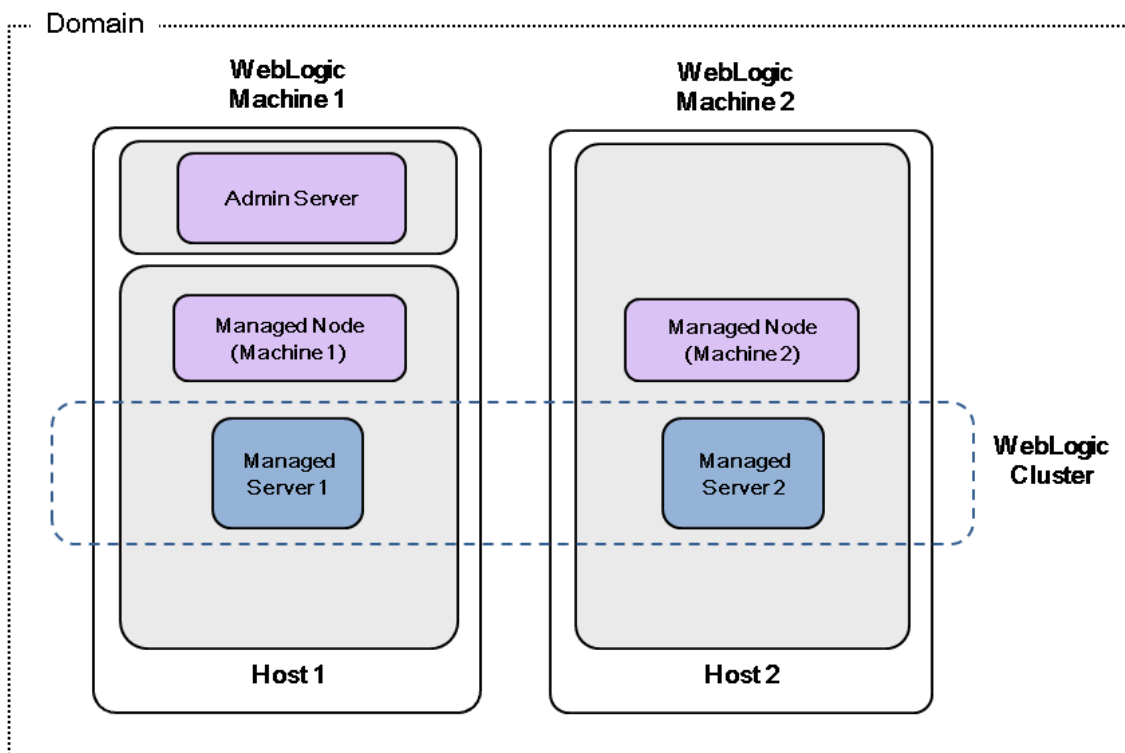
# Chapter 1: The WebLogic Provisioning Solution

The WebLogic provisioning solution provides tools that you can use to provision many features of a WebLogic 11g or 12c environment. These tools enable you to:

- Provision the WebLogic 11g or 12c software on the target host servers.
- Create a Node Manager to control the different WebLogic 11g or 12c Managed Servers.
- Provision the Administration Server.
- Create a WebLogic 11g or 12c domain.
- Provision Managed Servers.
- Control whether you want communications between WebLogic components via the more secure SSL communication with customized keystores and truststores.
- Create a cluster of Managed Servers.
- Control whether the cluster message mode is unicast or multicast.
- Expand the WebLogic 11g or 12c domain across multiple hosts.
- Modify an existing WebLogic domain to enable the domain-wide administration port.

The following reference architecture shows a simple WebLogic configuration:

### Oracle WebLogic 11g or 12c Provisioning



By consistently using the tools provided in this solution, you can quickly, efficiently, and accurately set up your entire WebLogic 11g or 12c environment. You maintain flexibility over the architecture by configuring environment-specific information through the input parameters.

## What this Solution Includes

The Application Server Provisioning solution pack contains the following WebLogic 11g or 12c provisioning workflows:

Workflow Name	Purpose
<a href="#">WebLogic - Create Trust and Identity Keystore</a>	This workflow uses the Java keytool to create a Java keystore, generate a key pair, and export the public key. Then the workflow creates a truststore and imports the public key into the newly created truststore. Finally, the workflow creates a certificate request that can be manually sent to a trusted Certificate Authority (CA) to be signed. After the signed certificate is received from the CA, you can manually import it into the existing truststore.
<a href="#">WebLogic - Provision Weblogic Software</a>	This workflow installs a new instance of Oracle WebLogic Server versions 11g or 12c onto the target host server (or servers) in silent mode with a response file. Either the native installer (the OS-specific package installer) or generic installer is used.
<a href="#">WebLogic - Provision Weblogic Domain and Admin Server</a>	This workflow creates a WebLogic domain and Administration Server from an existing installation of WebLogic 11g or 12c.
<a href="#">WebLogic - Provision Advanced Domain and Admin Server</a>	This workflow modifies an existing WebLogic domain and Administration Server, enables the domain-wide administration port, configures logging attributes of the domain and Administration Server, and modifies the WebLogic Scripting Tool (WLST) script to enable connection through the WLST to the domain-wide administration port.
<a href="#">WebLogic - Provision Weblogic Managed Servers</a>	This workflow creates a configuration for a WebLogic Managed Server (or servers) from an existing installation and domain of WebLogic.
<a href="#">Provision WebLogic Cluster</a>	This workflow creates a WebLogic cluster configuration from an existing installation and domain of WebLogic and adds the existing Managed Servers to the cluster configuration.
<a href="#">Increase WebLogic Domain Span</a>	This workflow increases the span of a WebLogic domain by adding other hosts to that domain. To accomplish this it moves the Managed Server configurations and cluster configuration to the other hosts, extends the cluster, starts the Managed Servers, and starts the cluster.

## Deprecated WebLogic Provisioning Workflows

The following workflows that are specifically for WebLogic have been deprecated from the solution pack and removed from the product:

Workflow Name	Purpose
Provision WebLogic Software	<p>This workflow installs a new instance of Oracle WebLogic Server versions 11g or 12c onto the target host server (or servers) in silent mode with a response file. Either the native installer (the OS-specific package installer) or generic installer is used.</p> <p>This workflow has been replaced by the <a href="#">WebLogic - Provision Weblogic Software</a> workflow.</p>
Provision WebLogic Domain and Admin Server	<p>This workflow creates a WebLogic domain and Administration Server from an existing installation of WebLogic.</p> <p>This workflow has been replaced by the <a href="#">WebLogic - Provision Weblogic Domain and Admin Server</a> workflow.</p>
Provision WebLogic Managed Servers	<p>This workflow creates a configuration for a WebLogic Managed Server (or servers) from an existing installation and domain of WebLogic.</p> <p>This workflow has been replaced by the <a href="#">WebLogic - Provision Weblogic Managed Servers</a> workflow.</p>

**Tip:** Documentation for deprecated workflows is available in the *HP DMA WebLogic Provisioning User Guide* for HP DMA version 10.10. This document is available on the HP Software Support web site: <https://softwaresupport.hp.com/>

# Supported Products and Platforms

## Operating Systems

The WebLogic 11g and 12c provisioning workflows are supported on the following operating system platforms:

- Red Hat Enterprise Linux
- SUSE Linux Enterprise Server
- Solaris

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

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

## Product Hardware and Software Requirements

For WebLogic 11g and 12c hardware and software requirements, see the [WebLogic Product Documentation](#) on page 125.

## HP DMA Hardware Requirements

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

## HP DMA Software Requirements

The latest HP DMA solution packs require the latest HP DMA platform. To use the latest solution packs, update the HP DMA platform. HP DMA 10.30 solution packs are supported on HP DMA 10.30 (and later).

# Prerequisites

The following prerequisites must be satisfied before you can run the WebLogic 11g and 12c provisioning workflows in this solution pack.

## **Database and Middleware Automation**

You have installed the Application Server Provisioning Solution Pack.

## **Memory**

You have a minimum of 1 GB RAM, although Oracle recommends at least 2 GB of RAM.

## **Hard disk drive**

A complete installation (including SDKs) requires approximately 3.9 GB of disk space. This includes temporary disk space that is needed during installation. Depending on the components you choose to install, and the installer that you are using, less disk space may be needed.

## **Processor**

You have a 1-GHz (or faster) CPU.

For more information about prerequisites for WebLogic 11g and 12c, refer to the [WebLogic Product Documentation](#) on page 125.

## Chapter 2: Workflow Details

The Application Server Provisioning solution pack contains the following WebLogic 11g or 12c provisioning workflows. You can run these workflows ad-hoc for custom WebLogic installations or create reusable deployments to standardize WebLogic installations in your environment.

Workflow Name	Purpose
<a href="#">WebLogic - Create Trust and Identity Keystore</a>	This workflow uses the Java keytool to create a Java keystore, generate a key pair, and export the public key. Then the workflow creates a truststore and imports the public key into the newly created truststore. Finally, the workflow creates a certificate request that can be manually sent to a trusted Certificate Authority (CA) to be signed. After the signed certificate is received from the CA, you can manually import it into the existing truststore.
<a href="#">WebLogic - Provision Weblogic Software</a>	This workflow installs a new instance of Oracle WebLogic Server versions 11g or 12c onto the target host server (or servers) in silent mode with a response file. Either the native installer (the OS-specific package installer) or generic installer is used.
<a href="#">WebLogic - Provision Weblogic Domain and Admin Server</a>	This workflow creates a WebLogic domain and Administration Server from an existing installation of WebLogic 11g or 12c.
<a href="#">WebLogic - Provision Advanced Domain and Admin Server</a>	This workflow modifies an existing WebLogic domain and Administration Server, enables the domain-wide administration port, configures logging attributes of the domain and Administration Server, and modifies the WebLogic Scripting Tool (WLST) script to enable connection through the WLST to the domain-wide administration port.
<a href="#">WebLogic - Provision Weblogic Managed Servers</a>	This workflow creates a configuration for a WebLogic Managed Server (or servers) from an existing installation and domain of WebLogic.
<a href="#">Provision WebLogic Cluster</a>	This workflow creates a WebLogic cluster configuration from an existing installation and domain of WebLogic and adds the existing Managed Servers to the cluster configuration.
<a href="#">Increase WebLogic Domain Span</a>	This workflow increases the span of a WebLogic domain by adding other hosts to that domain. To accomplish this it moves the Managed Server configurations and cluster configuration to the other hosts, extends the cluster, starts the Managed Servers, and starts the cluster.

Each workflow included in this solution pack has a set of input parameters whose values will be unique to your environment. If you provide correct values for the parameters that each scenario requires, the workflow will be able to accomplish its objective.

There are two steps required to customize this solution:

1. Ensure that all required parameters are visible. You do this by using the workflow editor.  
For simple provisioning scenarios, you can use the default values for most parameters. To use this solution's more advanced features, you will need to expose additional parameters.
2. Specify the values for those parameters. You do this when you create a deployment.

**Tip:** Detailed instructions are provided in the "How to Run this Workflow" topic associated with each workflow.

The information presented here assumes the following:

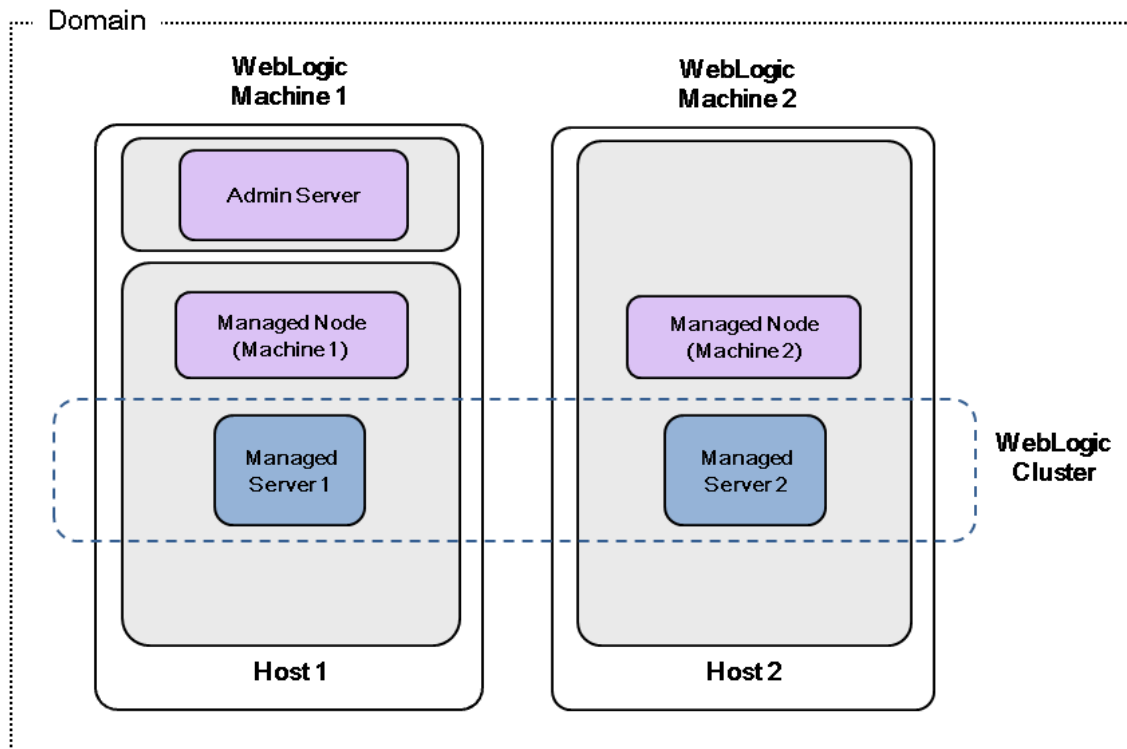
- HP DMA is installed and operational.
- At least one suitable target server is available (see [Supported Products and Platforms](#) on page 15).
- You are logged in to the HP DMA web interface.
- You have permission to create, edit, and deploy copies of the workflows included in this solution pack.

**Tip:** All parameters used by the workflows in this solution are described in the "Parameters" topic associated with each workflow.

## How to Use the Workflows Together

The workflows contained in the Application Server Provisioning Solution Pack are designed to work together to accomplish your provisioning tasks. You can create multiple topologies. The following reference architecture will be used throughout this guide to show the specific task that each workflow performs:

### Oracle WebLogic 11g or 12c Provisioning



### How to use the WebLogic provisioning workflows together:

1. *Optional:* If you plan to use SSL certificates, you can use the [WebLogic - Create Trust and Identity Keystore](#) workflow to set up the keystore and truststore, and to request a signed certificate from a trusted CA.
2. Use the [WebLogic - Provision Weblogic Software](#) workflow to lay down the WebLogic 11g or 12c binaries on all the target host servers that you plan to use in your WebLogic environment. Once you have the binaries on the servers, you can mold them to produce multiple configurations.
3. After the binaries are set up, use the [WebLogic - Provision Weblogic Domain and Admin Server](#) workflow to set up the process server and create the domain on the target host server where your Administration Server will reside. This workflow creates the box where the WebLogic components can be placed.
4. *Optional:* You can use the [WebLogic - Provision Advanced Domain and Admin Server](#) workflow to configure advanced features of the WebLogic domain and Administration Server, such as the domain-wide administration port.
5. After creating the process server and domain, use the [WebLogic - Provision Weblogic Managed Servers](#) workflow to create the configurations for the Managed Servers on the target host server where your Administration Server resides. Use the parameters to configure which Managed Servers go on which application servers. After this step you have a running environment.
6. *Optional:* You can use the [Provision WebLogic Cluster](#) workflow to put Managed Servers into a cluster configuration. You decide whether the cluster contains the Managed Servers from only one machine (a vertical cluster) or multiple machines (a horizontal cluster).
7. *Optional:* You can use the [Increase WebLogic Domain Span](#) workflow if you want the domain to span more than one machine. In other words, use this workflow if you have a horizontal cluster; it is not needed if you have a vertical cluster. To increase the domain, this workflow moves the Managed Server configurations and cluster configuration to the other hosts, extends the cluster, and then starts the Managed Servers in the cluster.

**Note:** If you do not plan to expand the domain, you should manually start the cluster after running the [Provision WebLogic Cluster](#) workflow.

# WebLogic - Create Trust and Identity Keystore

This workflow uses the Java keytool to create a Java keystore, generate a key pair, and export the public key. Then the workflow creates a truststore and imports the public key into the newly created truststore. Finally, the workflow creates a certificate request that can be manually sent to a trusted Certificate Authority (CA) to be signed. After the signed certificate is received from the CA, you can manually import it into the existing truststore.

**Tip:** This workflow is not exclusive to WebLogic. The workflow uses a generic Java keytool, allowing it to create the keystore and truststore for application servers, such as IBM WebSphere Application Server Network Deployment.

For information about how this workflow can be used with other WebLogicprovisioning workflows see [How to Use the Workflows Together](#) on page 19.

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

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

## Prerequisites for this Workflow

Be sure that the following prerequisites are satisfied before you run the [WebLogic - Create Trust and Identity Keystore](#) workflow:

- The latest HP DMA solution packs require the latest HP DMA platform. To use the latest solution packs, update the HP DMA platform. HP DMA 10.30 solution packs are supported on HP DMA 10.30 (and later).
- You have installed the Application Server Provisioning Solution Pack.
- This workflow is supported on the following Java installations: Java 1.6.x and Java 1.7.x

For more information about prerequisites for WebLogic 11g and 12c, refer to the [WebLogic Product Documentation](#) on page 125.

## How this Workflow Works

The following information describes how the [WebLogic - Create Trust and Identity Keystore](#) workflow works:

### Overview

The workflow does the following:

- Creates the Java keystore.
- Exports the public key out of the keystore and imports it into the truststore. Creates another file with the trusted certificates.
- Creates a certificate request that you can manually send to a Certificate Authority (CA).

**Note:** Most users wait to receive the signed certificate request back from the CA, but you can use a public certificate in the meantime.

- *Optional:* Imports the root CA certificate and the Intermediate Certificate into the truststore.

**Note:** If you do not import certificate when you run this workflow, you can also import it manually later.

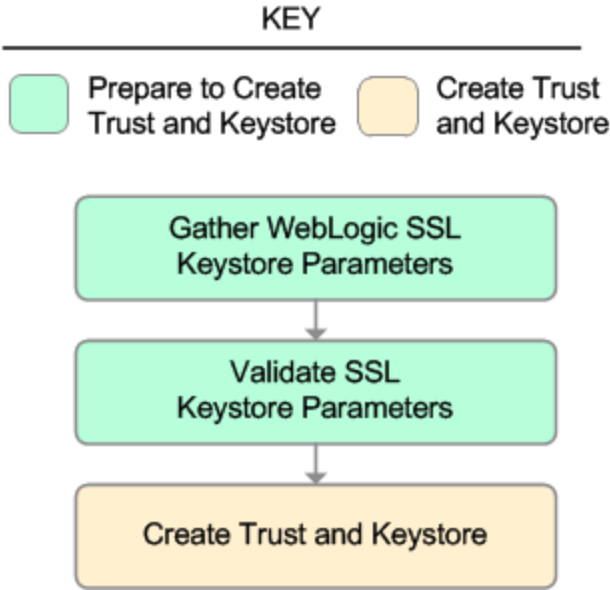
### Validation Checks Performed

Much of the validation centers on the input parameters:

- Required parameters have values specified.
- The Java Home version is 1.6 or greater.
- If Intermediate CA Alias is specified, Intermediate CA File Location is a valid existing path with a valid filename. If Intermediate CA File Location is specified, Intermediate CA Alias is specified.
- Certificate Location is a valid path.
- KeyStore Location Directory, Root CA File Location, and TrustStore Location are valid paths with valid filenames.
- KeySize and Validity are integers.

Steps Executed

The WebLogic - Create Trust and Identity Keystore workflow includes the following steps. Each step must complete successfully before the next step can start. If a step fails, the workflow reports a failure and all subsequent steps are skipped.



Steps Used in WebLogic - Create Trust and Identity Keystore

Workflow Step	Description
Gather WebLogic SSL Keystore Parameters	This step gathers all required parameters to create the SSL keystore, truststore, key pairs, exports/imports public key, to import the root CA and intermediate CA, and to create the certificate request.
Validate SSL Keystore Parameters	This step validates and prepares the parameters to create the SSL keystore, truststore, key pairs, exports/imports public key, to import the root CA and intermediate CA, and to create the certificate request.
Create Trust and Keystore	This step creates the SSL keystore, truststore, key pairs, and exports/imports public key. The step imports the root CA and intermediate CA. The step creates the certificate request.

For parameter descriptions and defaults, see [Parameters for WebLogic - Create Trust and Identity Keystore](#).

## How to Run this Workflow

The following instructions show you how to customize and run the [WebLogic - Create Trust and Identity Keystore](#) workflow in your environment.

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

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

**Note:** Before following this procedure, review the [Prerequisites for this Workflow](#) on page 22, and ensure that all requirements are satisfied.

### To use the WebLogic - Create Trust and Identity Keystore workflow:

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

#### Input Parameters for Gather WebLogic SSL Keystore Parameters

Parameter Name	Default Value	Required	Description
Cert Location	no default	required	Fully qualified directory path where the certificate and certificate request will be created. For example: /opt/app/ssl/
Dname Suffix	no default	required	The suffix of the Distinguished Name (DN) that will uniquely identify an entity in an X.509 certificate. The CN will be generated from the server name. For example: OU=Software, O=HP, L=Fort Collins, ST=Colorado, C=US
Intermediate CA Alias	no default	optional	Name or label to uniquely identify the Intermediate CA in the truststore. For example: intermediateca
Intermediate CA File Location	no default	optional	Fully qualified file path where the Intermediate CA is located. For example: /opt/app/ssl/intermediateca.crt
Java Home	no default	required	Fully qualified path to the JAVA_HOME that the keytool uses to create the SSL configuration. For example: /opt/app/jdk1.6.0_35

### Input Parameters for Gather WebLogic SSL Keystore Parameters, continued

Parameter Name	Default Value	Required	Description
KeySize	2048	required	Key size or length (in bits) that will be used when creating the Java keystore. For example: 2048
KeyStore Location	no default	required	Fully qualified directory path where the Java keystore will be created. For example: /opt/app/ssl
KeyStore Passphrase	no default	required	Keystore password used to create the keystore and export certificate.
PrivateKey Passphrase	no default	required	Password used to protect the private key in the keystore.
Root CA Alias	no default	required	Name or label to uniquely identify the Root CA in the truststore. For example: rootca
Root CA File Location	no default	required	Fully qualified file path where the Root CA is located. For example: /opt/app/ssl/rootca.crt
TrustStore Location	no default	required	Fully qualified directory path where the Java truststore will be created. For example: /opt/app/ssl
Validity	no default	required	The number of days that the certificate is valid. For example: 365

**Tip:** To avoid having to re-enter passwords whenever they change, you can create a policy to provide them to the workflow (see [How to Use a Policy to Specify Parameter Values](#) on page 132).

**Note:** See [Parameters for WebLogic - Provision Weblogic Software](#) for detailed descriptions of all input parameters for this workflow, including default values.

3. In the workflow editor, expose any additional parameters that you need. You will specify values for those parameters when you create the deployment.
4. Save the changes to the workflow (click **Save** in the lower right corner).
5. Create a new deployment (see "Create a Deployment" in *HP DMA Quick Start Tutorial* for instructions).
6. On the Parameters tab, specify values for the required parameters listed in step 2 and any additional parameters that you have exposed. You do not need to specify values for those parameters whose default values are appropriate for your environment.

7. On the Targets tab, specify one or more targets for this deployment.

**Note:** The target for this deployment should be set to all the servers that are involved in your WebLogic installation.

8. Save the deployment (click **Save** in the lower right corner).
9. Run the workflow using this deployment (see "Run Your Workflow" in *HP DMA Quick Start Tutorial* for instructions).

**To verify the results:**

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

*Optional:* If you want to further verify the results:

Make sure that the keystore, truststore, public key, and certificate request exist.

**To do after running this workflow:**

Submit the certificate signing request to your CA. The CA will provide instructions for submitting this request.

In response to your request, the CA will send you a digitally signed server certificate via email. Your CA may also send you the root certificate and any intermediate certificates required. Your CA will provide instructions for importing the root and any intermediate certificates into the keystore.

## Sample Scenario

It is very straightforward to run the [WebLogic - Create Trust and Identity Keystore](#) workflow. This topic shows you typical parameter values to use.

### Typical parameters

#### Input Parameters for Gather WebLogic SSL Keystore Parameters

Parameter Name	Example Value	Description
Cert Location	see description	Fully qualified directory path where the certificate and certificate request will be created.  For example: /opt/app/ssl/
Dname Suffix	see description	The suffix of the Distinguished Name (DN) that will uniquely identify an entity in an X.509 certificate. The CN will be generated from the server name.  For example: OU=Software, O=HP, L=Fort Collins, ST=Colorado, C=US
Intermediate CA Alias	intermediateca	Name or label to uniquely identify the Intermediate CA in the truststore.  For example: intermediateca
Intermediate CA File Location	see description	Fully qualified file path where the Intermediate CA is located.  For example: /opt/app/ssl/intermediateca.crt
Java Home	see description	Fully qualified path to the JAVA_HOME that the keytool uses to create the SSL configuration.  For example: /opt/app/jdk1.6.0_35
KeySize	2048	Key size or length (in bits) that will be used when creating the Java keystore.  For example: 2048
KeyStore Location	/opt/app/ssl	Fully qualified directory path where the Java keystore will be created.  For example: /opt/app/ssl
KeyStore Passphrase	kspassword	Keystore password used to create the keystore and export certificate.
PrivateKey Passphrase	pkpassword	Password used to protect the private key in the keystore.

#### Input Parameters for Gather WebLogic SSL Keystore Parameters, continued

Parameter Name	Example Value	Description
Root CA Alias	rootca	Name or label to uniquely identify the Root CA in the truststore. For example: rootca
Root CA File Location	see description	Fully qualified file path where the Root CA is located. For example: /opt/app/ssl/rootca.crt
TrustStore Location	/opt/app/ssl	Fully qualified directory path where the Java truststore will be created. For example: /opt/app/ssl
Validity	365	The number of days that the certificate is valid. For example: 365

Be sure that the default values for all remaining input parameters are appropriate for your environment (see [Parameters for WebLogic - Create Trust and Identity Keystore](#)).

## Parameters for WebLogic - Create Trust and Identity Keystore

The following tables describe the required and optional input parameters for this workflow. Some of these parameters may not be initially visible in a deployment (see [How to Expose Additional Workflow Parameters](#) on page 131). For some parameters, if you do not specify a value for a parameter, a default value is assigned.

Following is a table for the sole step used by this workflow where parameters are defined:

Parameters Defined in this Step: Gather WebLogic SSL Keystore Parameters

Parameter Name	Default Value	Required	Description
Cert Location	no default	required	Fully qualified directory path where the certificate and certificate request will be created.  For example: /opt/app/ssl/
Dname Suffix	no default	required	The suffix of the Distinguished Name (DN) that will uniquely identify an entity in an X.509 certificate. The CN will be generated from the server name.  For example: OU=Software, O=HP, L=Fort Collins, ST=Colorado, C=US
Hostname	Server.Name	required	The host name or IP address used to create the CN or common name.  For example: myserver.mycompany.com
Intermediate CA Alias	no default	optional	Name or label to uniquely identify the Intermediate CA in the truststore.  For example: intermediateca
Intermediate CA File Location	no default	optional	Fully qualified file path where the Intermediate CA is located.  For example: /opt/app/ssl/intermediateca.crt
Java Home	no default	required	Fully qualified path to the JAVA_HOME that the keytool uses to create the SSL configuration.  For example: /opt/app/jdk1.6.0_35
KeySize	2048	required	Key size or length (in bits) that will be used when creating the Java keystore.  For example: 2048

Parameters Defined in this Step: Gather WebLogic SSL Keystore Parameters, continued

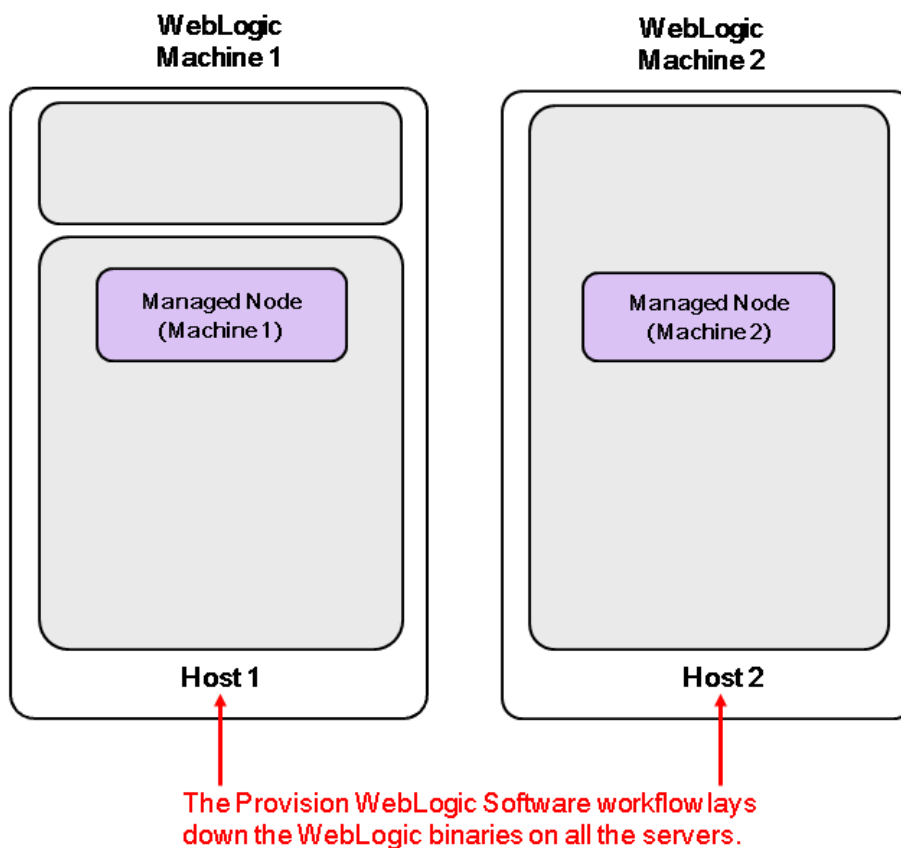
Parameter Name	Default Value	Required	Description
KeyStore Location	no default	required	Fully qualified directory path where the Java keystore will be created.  For example: /opt/app/ssl
KeyStore Passphrase	no default	required	Keystore password used to create the keystore and export certificate.
PrivateKey Passphrase	no default	required	Password used to protect the private key in the keystore.
Root CA Alias	no default	required	Name or label to uniquely identify the Root CA in the truststore.  For example: rootca
Root CA File Location	no default	required	Fully qualified file path where the Root CA is located.  For example: /opt/app/ssl/rootca.crt
TrustStore Location	no default	required	Fully qualified directory path where the Java truststore will be created.  For example: /opt/app/ssl
Validity	no default	required	The number of days that the certificate is valid.  For example: 365

## WebLogic - Provision Weblogic Software

This workflow installs a new instance of Oracle WebLogic Server versions 11g or 12c onto the target host server (or servers) in silent mode with a response file. Either the native installer (the OS-specific package installer) or generic installer is used.

This workflow supports WebLogic 11g and 12c with either the native installer or the generic installer. The end user specifies whether or not to start the Node Manager. The workflow modifies the Node Manager property file to enable and configure custom SSL connectivity.

The following reference architecture diagram gives an example of what this workflow does:



For information about how this workflow can be used with other WebLogic provisioning workflows see [How to Use the Workflows Together](#) on page 19.

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

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

**Note:** The documentation for this workflow refers to the workflow and its steps by their base names. The names in the HP DMA user interface may have a version appended, for example, v2.

## Prerequisites for this Workflow

Be sure that the following prerequisites are satisfied before you run the [WebLogic - Provision Weblogic Software](#) workflow:

- The latest HP DMA solution packs require the latest HP DMA platform. To use the latest solution packs, update the HP DMA platform. HP DMA 10.30 solution packs are supported on HP DMA 10.30 (and later).
- You have installed the Application Server Provisioning Solution Pack.
- You have a support contract and have downloaded the appropriate WebLogic 11g and 12c software to software repository or to the target machine.
- If the generic installer is to be used, you must already have a JDK (Java development kit)—supported by the version of WebLogic you are installing—installed on the target machine.

### Memory

A minimum of 1 GB RAM, although Oracle recommends 2 GB of RAM.

### Hard disk drive

A complete installation (including SDKs) requires approximately 3.9 GB of disk space. This includes temporary disk space that is needed during installation. Depending on the components you choose to install, and the installer that you are using, less disk space may be needed.

### Processor

1-GHz (or faster) CPU

For more information about prerequisites for WebLogic 11g and 12c, refer to the [WebLogic Product Documentation](#) on page 125.

## How this Workflow Works

The following information describes how the [WebLogic - Provision Weblogic Software](#) workflow works:

### Overview

The workflow does the following:

- Prepares to provision the WebLogic software on all target machines by setting up the command to be used in subsequent steps, validating input parameters, verifying that the operating system is supported, and determining that enough temporary storage space is available.
- Checks the existence of the binary executable file, downloads it from the software repository if it doesn't exist, then changes the file ownership and permissions so that it can be executed.
- Creates the response file that is required to drive the WebLogic installation.
- Depending on the Java Home parameter:
  - If the Java Home parameter is specified, the workflow uses the generic package installer—the JDK utility located at Java Home—to lay down the WebLogic binaries onto the target host server using silent mode and the specified response file.
  - If the Java Home parameter is not specified, the workflow uses the OS-specific package installer to lay down the WebLogic binaries onto the target host server using silent mode and the specified response file.
- *Optional:* Starts the WebLogic Node Manager process on the target host servers.
- *Optional:* Configures the Custom SSL configurations for the WebLogic Node Manager. Stops and restarts the WebLogic Node Manager to apply the SSL configuration changes.
- Cleans up any files that were downloaded—for either workflow success or failure.

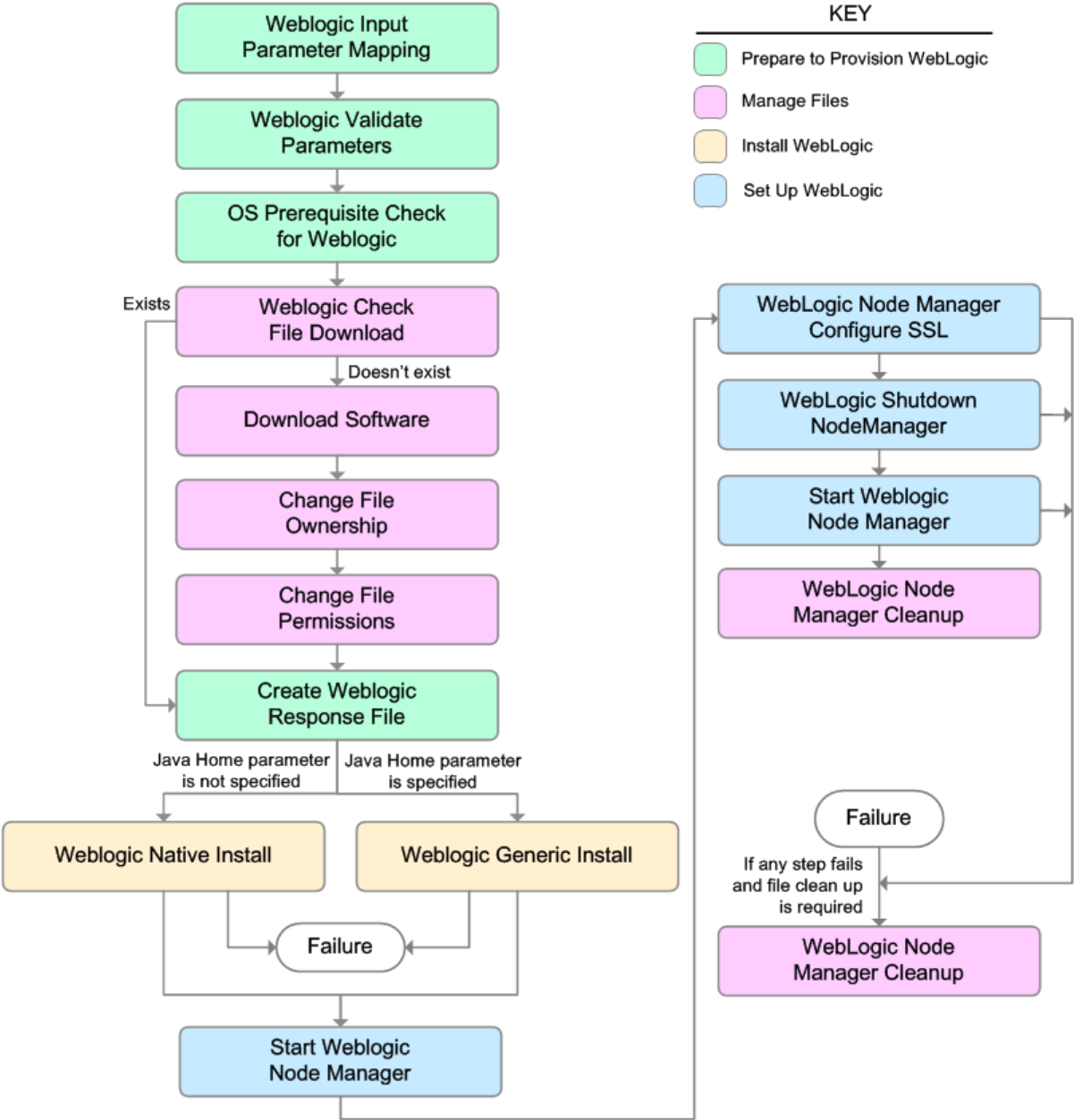
### Validation Checks Performed

Much of the validation centers on the input parameters:

- Required parameters have values specified.
- The Binary Archive file or path is valid.
- The Java Home, Staging Directory, NM Log File are valid.
- The Node Manager Service, Setup Custom SSL Stores, and Start Node Manager parameters are either true or false.
- The Node Manager Port is either null or a valid integer.
- The Binary Archive and Java Home are valid install files.
- If Setup Custom SSL Stores is true, the following parameters are specified: Custom KeyStore PassPhrase, Custom KeyStore Path, Custom KeyStore Type, Custom PrivateKey PassPhrase, Custom TrustStore Path, and Private Key Alias.
- The WebLogic User and WebLogic Group exist and the WebLogic User is part of the specified WebLogic Group.

Steps Executed

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



## Steps Used in WebLogic - Provision Weblogic Software

Workflow Step	Description
Weblogic Input Parameter Mapping	<p>This step performs the following actions to facilitate the execution of subsequent steps in the workflow:</p> <ol style="list-style-type: none"> <li>1. Sets the Call Wrapper parameter to its default value. The Call Wrapper is the command that executes a step as a specific user.</li> <li>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.</li> </ol>
Weblogic Validate Parameters	This step prepares and validates the input parameters required to install WebLogic.
OS Prerequisite Check for Weblogic	This step first determines whether the operating system kernel on the target server is a supported version, and then it determines if adequate temporary space is available to extract the contents of the installation binaries and install WebLogic.
Weblogic Check File Download	<p>This step checks for the existence of a file on the target machine before downloading that file from the software repository. For each file in the specified File List, it:</p> <ol style="list-style-type: none"> <li>1. Determines whether the file is in the expected location on the target machine.</li> <li>2. If the file is not in the expected location, adds that file to a list of files that need to be downloaded.</li> </ol>
Download Software	This step downloads a list of files to a specified location on the target server.
Change File Ownership	This step changes the ownership of a comma-delimited list of files to the specified user and group.
Change File Permissions	This step changes the permissions settings for one or more specified files or directories.
Create Weblogic Response File	This step creates the response file required to drive the installation of WebLogic and determines whether the generic or native installer will be used.
Weblogic Native Install	This step starts the installation of WebLogic using the native installer—OS-package specific—with silent mode and the specified response file.
Weblogic Generic Install	This step starts the installation of WebLogic using the generic installer—JDK utility—with silent mode and the specified response file.

Steps Used in WebLogic - Provision Weblogic Software, continued

Workflow Step	Description
Start Weblogic Node Manager	This step checks if Start Node Manager is set to true. If so, it starts the WebLogic Node Manager process on the target server. Then the step verifies that the Node Manager started.
WebLogic Node Manager Configure SSL	This step updates the <code>nodemanager.properties</code> file with the SSL configurations and changes the Node Manager log file location.
WebLogic Shutdown NodeManager	This step stops the WebLogic Node Manager on a given machine or server.
Start Weblogic Node Manager	This step checks if Start Node Manager is set to true. If so, it starts the WebLogic Node Manager process on the target server. Then the step verifies that the Node Manager started.
WebLogic Node Manager Cleanup	This step removes all temporary downloaded files and archives.

For parameter descriptions and defaults, see [Parameters for WebLogic - Provision Weblogic Software](#).

## How to Run this Workflow

The following instructions show you how to customize and run the [WebLogic - Provision Weblogic Software](#) workflow in your environment.

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

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

**Note:** Before following this procedure, review the [Prerequisites for this Workflow](#) on page 34, and ensure that all requirements are satisfied.

### To use the WebLogic - Provision Weblogic Software workflow:

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

#### Input Parameters for Weblogic Validate Parameters

Parameter Name	Default Value	Required	Description
BEA Home	no default	required	Fully qualified path to the middleware home directory that will contain this installation. For example: <code>/opt/oracle/weblogic</code>
Binary Archive	no default	required	Fully qualified path to the WebLogic Package Installer. Not required if Java Binary Archive is provided.

### Input Parameters for Weblogic Validate Parameters, continued

Parameter Name	Default Value	Required	Description
Component Paths	see description	required	<p>The components and/or subcomponents that you want to install on your system. To install multiple components, separate the components with a bar   character. Default is:</p> <p>WebLogic Server/Core Application Server    WebLogic Server/Administration Console    WebLogic Server/Configuration Wizard and Upgrade Framework    WebLogic Server/Web 2.0 HTTP Pub-Sub Server    WebLogic Server/WebLogic JDBC Drivers    WebLogic Server/Third Party JDBC Drivers    WebLogic Server/WebLogic Server Clients    WebLogic Server/WebLogic Web Server Plugins    WebLogic Server/UDDI and Xquery Support    WebLogic Server/Server Examples</p> <p><b>Note:</b> If you specify WebLogic Server, you will install all of the above.</p>
Java Home	no default	required if generic installer is used	<p>Fully qualified path to the JAVA_HOME—JDK utility—that will be used for the generic install. For example:</p> <p>/opt/oracle/jdk1.6.0_35</p>
Log File	no default	required	<p>The fully qualified path where a verbose log file will be generated during installation. For example:</p> <p>/var/tmp/weblogic_log.txt</p>
Setup Custom SSL Stores	no default	required	<p>Determines whether you want to run Secure Socket Layer (SSL) with the demo SSL certificates or with your own custom keystore and truststore. Valid values are true or false.</p> <p>If Setup Custom SSL Stores is true, the following parameters must also be specified: Custom KeyStore PassPhrase, Custom KeyStore Path, Custom KeyStore Type, Custom PrivateKey PassPhrase, Custom TrustStore Path, and Private Key Alias.</p>
Staging Directory	no default	required	<p>Fully qualified path to a temporary directory that the installer will use to uncompress the binary into.</p>
Start Node Manager	true	required	<p>Determines whether to start the WebLogic Node Manager. Valid values are true and false.</p>

#### Input Parameters for Weblogic Validate Parameters, continued

Parameter Name	Default Value	Required	Description
WLS Install Home	no default	required	Fully qualified path to the directory where WebLogic Server will be installed. For example: <code>/opt/oracle/weblogic/wlserver12.1</code>
Weblogic Group	see description	optional	Group ID used to install the WebLogic software. The default is the group ID of root.
Weblogic User	root	optional	User ID used to install the WebLogic software.

**Tip:** To avoid having to re-enter passwords whenever they change, you can create a policy to provide them to the workflow (see [How to Use a Policy to Specify Parameter Values](#) on page 132).

**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 [How to Expose Additional Workflow Parameters](#) on page 131

See [Parameters for WebLogic - Provision Weblogic Software](#) for detailed descriptions of all input parameters for this workflow, including default values.

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

**Note:** The target for this deployment should be set to all the servers that are involved in your WebLogic installation.

8. Save the deployment (click **Save** in the lower right corner).
9. Run the workflow using this deployment (see "Run Your Workflow" in *HP DMA Quick Start Tutorial* for instructions).

#### To verify the results:

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

*Optional:* If you want to further verify the results:

View the `{BEAHOME}/logs/log.txt` file. This file is created after the installation and contains specific information about what was installed.

## Sample Scenario

This topic shows you typical parameter values for different use cases for the [WebLogic - Provision Weblogic Software](#) workflow.

### Scenario 1: Use the native installer and install WebLogic as a non-root user

If you want to use the native—OS-specific—package installer to lay down the WebLogic binaries onto the target host server, do not set the Java Home parameter.

Set Setup Custom SSL Stores to false.

#### Input Parameters for Weblogic Validate Parameters

Parameter Name	Example Value	Description
BEA Home	see description	Fully qualified path to the middleware home directory that will contain this installation. For example:  <code>/opt/oracle/weblogic</code>
Binary Archive	<code>wls_1035_linux.bin</code>	Fully qualified path to the WebLogic Package Installer. Not required if Java Binary Archive is provided.
Component Paths	WebLogic Server (this installs everything under it)	<p>The components and/or subcomponents that you want to install on your system. To install multiple components, separate the components with a bar   character. Default is:</p> <p>WebLogic Server/Core Application Server    WebLogic Server/Administration Console    WebLogic Server/Configuration Wizard and Upgrade Framework    WebLogic Server/Web 2.0 HTTP Pub-Sub Server    WebLogic Server/WebLogic JDBC Drivers    WebLogic Server/Third Party JDBC Drivers    WebLogic Server/WebLogic Server Clients    WebLogic Server/WebLogic Web Server Plugins    WebLogic Server/UDDI and Xquery Support    WebLogic Server/Server Examples</p> <p><b>Note:</b> If you specify WebLogic Server, you will install all of the above.</p>
Java Home		Fully qualified path to the JAVA_HOME—JDK utility—that will be used for the generic install. For example:  <code>/opt/oracle/jdk1.6.0_35</code>
Log File	<code>/tmp/weblogic_log.txt</code>	The fully qualified path where a verbose log file will be generated during installation. For example:  <code>/var/tmp/weblogic_log.txt</code>

### Input Parameters for Weblogic Validate Parameters, continued

Parameter Name	Example Value	Description
Setup Custom SSL Stores	false	Determines whether you want to run Secure Socket Layer (SSL) with the demo SSL certificates or with your own custom keystore and truststore. Valid values are true or false.  If Setup Custom SSL Stores is true, the following parameters must also be specified: Custom KeyStore PassPhrase, Custom KeyStore Path, Custom KeyStore Type, Custom PrivateKey PassPhrase, Custom TrustStore Path, and Private Key Alias.
Staging Directory	/tmp/	Fully qualified path to a temporary directory that the installer will use to uncompress the binary into.
Start Node Manager	true	Determines whether to start the WebLogic Node Manager. Valid values are true and false.
WLS Install Home	see description	Fully qualified path to the directory where WebLogic Server will be installed. For example:  /opt/oracle/weblogic/wlserver12.1
Weblogic Group	wlsgrp	Group ID used to install the WebLogic software. The default is the group ID of root.
Weblogic User	wlsuser	User ID used to install the WebLogic software.

Be sure that the default values for all remaining input parameters are appropriate for your environment (see [Parameters for WebLogic - Provision Weblogic Software](#)).

## Scenario 2: Use the generic installer, configure SSL with a custom keystore and truststore, and install WebLogic as a non-root user

If you want to use the generic package installer to lay down the WebLogic binaries onto the target host server, set the Java Home parameter to the JDK utility location.

Use this case to set up SSL to have the Node Manager communicate via SSL. Set Setup Custom SSL Stores to true. Also provide values for the following parameters: Custom KeyStore PassPhrase, Custom KeyStore Path, Custom KeyStore Type, Custom PrivateKey PassPhrase, Custom TrustStore Path, and Private Key Alias.

### Input Parameters for WebLogic Validate Parameters

Parameter Name	Example Value	Description
BEA Home	see description	Fully qualified path to the middleware home directory that will contain this installation. For example:  <code>/opt/oracle/weblogic</code>
Binary Archive	<code>wls_1035_linux.bin</code>	Fully qualified path to the WebLogic Package Installer. Not required if Java Binary Archive is provided.
Component Paths	WebLogic Server (this installs everything under it)	<p>The components and/or subcomponents that you want to install on your system. To install multiple components, separate the components with a bar   character. Default is:</p> <p>WebLogic Server/Core Application Server    WebLogic Server/Administration Console    WebLogic Server/Configuration Wizard and Upgrade Framework    WebLogic Server/Web 2.0 HTTP Pub-Sub Server    WebLogic Server/WebLogic JDBC Drivers    WebLogic Server/Third Party JDBC Drivers    WebLogic Server/WebLogic Server Clients    WebLogic Server/WebLogic Web Server Plugins    WebLogic Server/UDDI and Xquery Support    WebLogic Server/Server Examples</p> <p><b>Note:</b> If you specify WebLogic Server, you will install all of the above.</p>
Custom KeyStore PassPhrase	password	Password for the custom keystore.
Custom KeyStore Path	<code>/opt/WebLogic/keystore</code>	Fully qualified path to the custom keystore file.

### Input Parameters for WebLogic Validate Parameters, continued

Parameter Name	Example Value	Description
Custom KeyStore Type	JKS	The type of the Identity keystore.
Custom PrivateKey PassPhrase	password	Password used to retrieve the private key for the WebLogic Server from the Identity keystore.
Custom TrustStore Path	/opt/WebLogic/truststore	Fully qualified path to the custom truststore file.
Java Home	see description	Fully qualified path to the JAVA_HOME—JDK utility—that will be used for the generic install. For example:  /opt/oracle/jdk1.6.0_35
Log File	/tmp/weblogic_log.txt	The fully qualified path where a verbose log file will be generated during installation. For example:  /var/tmp/weblogic_log.txt
Private Key Alias	Hostname	The keystore attribute that defines the string alias used to store and retrieve the server's private key.
Setup Custom SSL Stores	true	Determines whether you want to run Secure Socket Layer (SSL) with the demo SSL certificates or with your own custom keystore and truststore. Valid values are true or false.  If Setup Custom SSL Stores is true, the following parameters must also be specified: Custom KeyStore PassPhrase, Custom KeyStore Path, Custom KeyStore Type, Custom PrivateKey PassPhrase, Custom TrustStore Path, and Private Key Alias.
Staging Directory	/tmp/	Fully qualified path to a temporary directory that the installer will use to uncompress the binary into.
Start Node Manager	true	Determines whether to start the WebLogic Node Manager. Valid values are true and false.
WLS Install Home	see description	Fully qualified path to the directory where WebLogic Server will be installed. For example:  /opt/oracle/weblogic/wlserver12.1
Weblogic Group	wlsgrp	Group ID used to install the WebLogic software. The default is the group ID of root.
Weblogic User	wlsuser	User ID used to install the WebLogic software.

**Note:** Some of these parameters are not exposed by default in the deployment. See [How to Expose Additional Workflow Parameters](#) on page 131.

You need to expose the following parameters: Custom KeyStore PassPhrase, Custom KeyStore Path, Custom KeyStore Type, Custom PrivateKey PassPhrase, Custom TrustStore Path, Node Manager Service, and Private Key Alias.

Be sure that the default values for all remaining input parameters are appropriate for your environment (see [Parameters for WebLogic - Provision Weblogic Software](#)).

## Parameters for WebLogic - Provision Weblogic Software

The following tables describe the required and optional input parameters for this workflow. Some of these parameters may not be initially visible in a deployment (see [How to Expose Additional Workflow Parameters](#) on page 131). For some parameters, if you do not specify a value for a parameter, a default value is assigned.

Following is a table for the sole step used by this workflow where parameters are defined:

Parameters Defined in this Step: Weblogic Validate Parameters

Parameter Name	Default Value	Required	Description
BEA Home	no default	required	Fully qualified path to the middleware home directory that will contain this installation. For example:  <code>/opt/oracle/weblogic</code>
Binary Archive	no default	required	Fully qualified path to the WebLogic Package Installer. Not required if Java Binary Archive is provided.
Call Wrapper	see description	optional	Command that will execute this step (or subsequent steps) as a specific user.  For UNIX targets, the default is: <code>/opt/hp/dma/client/jython.sh</code> running as root  For Windows targets, the default is: <code>jython</code> running as Administrator  <b>Caution:</b> This parameter is derived by the workflow. Under most circumstances, you should not change its mapping or its value.

Parameters Defined in this Step: Weblogic Validate Parameters, continued

Parameter Name	Default Value	Required	Description
Component Paths	see description	required	<p>The components and/or subcomponents that you want to install on your system. To install multiple components, separate the components with a bar   character. Default is:</p> <p>WebLogic Server/Core Application Server    WebLogic Server/Administration Console    WebLogic Server/Configuration Wizard and Upgrade Framework    WebLogic Server/Web 2.0 HTTP Pub-Sub Server    WebLogic Server/WebLogic JDBC Drivers    WebLogic Server/Third Party JDBC Drivers    WebLogic Server/WebLogic Server Clients    WebLogic Server/WebLogic Web Server Plugins    WebLogic Server/UDDI and Xquery Support    WebLogic Server/Server Examples</p> <p><b>Note:</b> If you specify WebLogic Server, you will install all of the above.</p>
Custom KeyStore PassPhrase	no default	optional	Password for the custom keystore.
Custom KeyStore Path	no default	optional	Fully qualified path to the custom keystore file.
Custom KeyStore Type	JKS	optional	The type of the Identity keystore.
Custom PrivateKey PassPhrase	no default	optional	Password used to retrieve the private key for the WebLogic Server from the Identity keystore.
Custom TrustStore Path	no default	optional	Fully qualified path to the custom truststore file.
Java Home	no default	required if generic installer is used	<p>Fully qualified path to the JAVA_HOME—JDK utility—that will be used for the generic install. For example:</p> <p>/opt/oracle/jdk1.6.0_35</p>

Parameters Defined in this Step: Weblogic Validate Parameters, continued

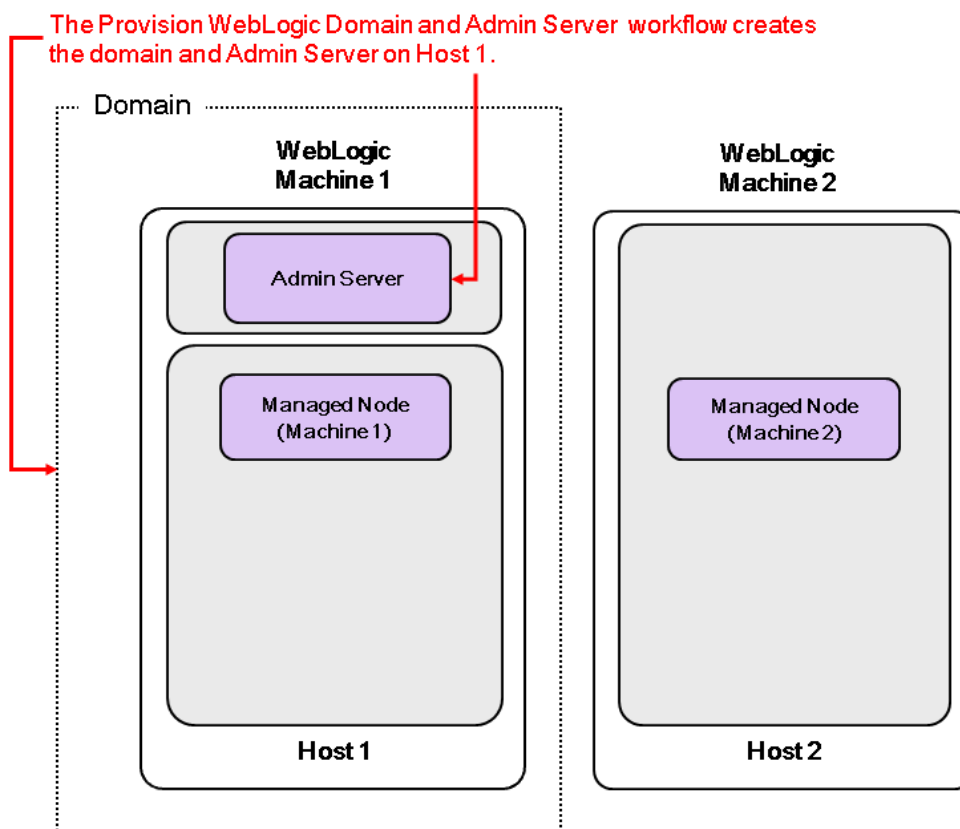
Parameter Name	Default Value	Required	Description
Log File	no default	required	The fully qualified path where a verbose log file will be generated during installation. For example:  <code>/var/tmp/weblogic_log.txt</code>
NM Log File	no default	optional	The fully qualified path where a Node Manager log file will be generated during installation.
Node Manager Port	5556	optional	Sets the port number under which the Node Manager will run.
Node Manager Service	false	required	Provides the option to set the Node Manager to run as a Windows Service. Valid values are true or false.
Private Key Alias	no default	optional	The keystore attribute that defines the string alias used to store and retrieve the server's private key.
Setup Custom SSL Stores	no default	required	Determines whether you want to run Secure Socket Layer (SSL) with the demo SSL certificates or with your own custom keystore and truststore. Valid values are true or false.  If Setup Custom SSL Stores is true, the following parameters must also be specified: Custom KeyStore PassPhrase, Custom KeyStore Path, Custom KeyStore Type, Custom PrivateKey PassPhrase, Custom TrustStore Path, and Private Key Alias.
Staging Directory	no default	required	Fully qualified path to a temporary directory that the installer will use to uncompress the binary into.
Start Node Manager	true	required	Determines whether to start the WebLogic Node Manager. Valid values are true and false.
WLS Install Home	no default	required	Fully qualified path to the directory where WebLogic Server will be installed. For example:  <code>/opt/oracle/weblogic/wlserver12.1</code>
Weblogic Group	see description	optional	Group ID used to install the WebLogic software. The default is the group ID of root.
Weblogic User	root	optional	User ID used to install the WebLogic software.

## WebLogic - Provision Weblogic Domain and Admin Server

This workflow creates a WebLogic domain and Administration Server from an existing installation of WebLogic 11g or 12c.

After you have the WebLogic 11g or 12c binaries installed, this workflow sets up the process server and creates the domain where the components can be placed.

The following reference architecture diagram gives an example of what this workflow does:



For information about how this workflow can be used with other WebLogic provisioning workflows see [How to Use the Workflows Together](#) on page 19.

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

Topic	Information Included
<a href="#">Prerequisites for this Workflow</a>	List of prerequisites that must be satisfied before you can run this workflow
<a href="#">How this Workflow Works</a>	Information about what the workflow does, including validation checks performed, steps executed, and a high-level process flow
<a href="#">How to Run this Workflow</a>	Instructions for running this workflow in your environment
<a href="#">Sample Scenario</a>	Examples of typical parameter values for this workflow
<a href="#">Parameters</a>	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 HP DMA user interface may have a version appended, for example, v2.

## Prerequisites for this Workflow

Be sure that the following prerequisites are satisfied before you run the [WebLogic - Provision Weblogic Domain and Admin Server](#) workflow:

1. The latest HP DMA solution packs require the latest HP DMA platform. To use the latest solution packs, update the HP DMA platform. HP DMA 10.30 solution packs are supported on HP DMA 10.30 (and later).
2. You have installed the Application Server Provisioning Solution Pack.

For more information about prerequisites for WebLogic 11g and 12c, refer to the [WebLogic Product Documentation](#) on page 125.

## How this Workflow Works

The following information describes how the [WebLogic - Provision Weblogic Domain and Admin Server](#) workflow works:

### Overview

The workflow does the following:

- Prepares to provision the WebLogic domain and Administration Server by setting up the command to be used in subsequent steps and validating input parameters.
- Creates the domain and Administration Server using the WebLogic Scripting Tool (WLST). To do this the workflow opens a domain template, configures the Administration Server and SSL port, writes the domain, then closes the domain template.
- Starts the WebLogic Administration Manager process on the target host server.

### Validation Checks Performed

Much of the validation centers on the input parameters:

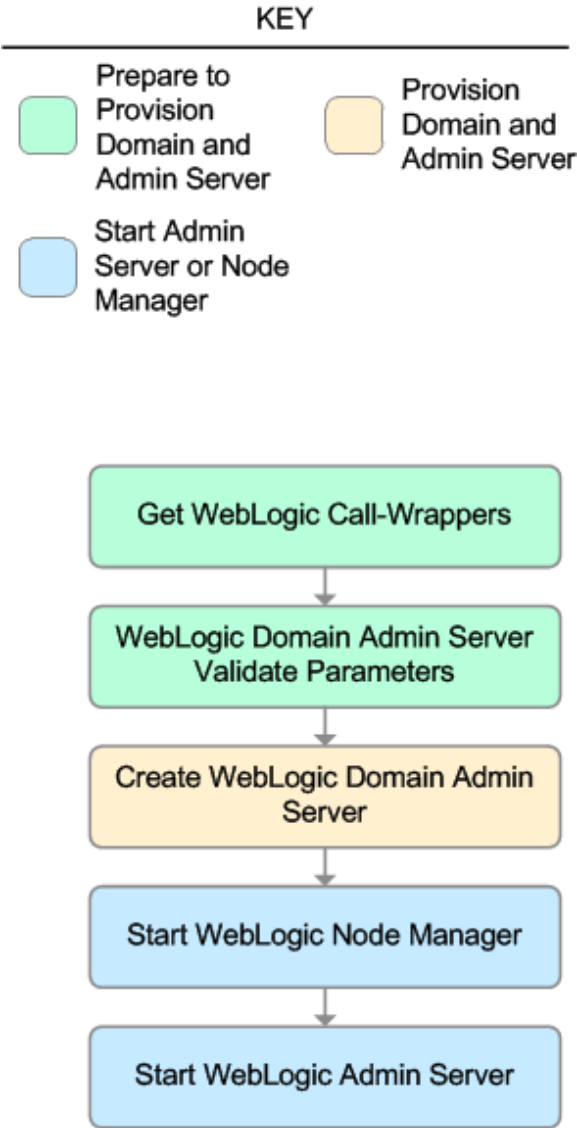
- Verifies that required parameters have values specified.
- Checks that the BEA Home and WLS Install Home files exist.
- Verifies that Admin Server Port and Admin SSL Port are null or valid integers.
- Verifies that Enable SSL, Setup Custom SSL Stores, and Start Node Manager are either true or false.
- Verifies that if Enable SSL is true that Setup Custom SSL Stores is also true.
- Verifies that if Enable SSL is true that Admin SSL Port has a value and if Enable SSL is false that Admin SSL Port does not have a value.
- If Setup Custom SSL Stores is true:

Verifies that the following are specified: Custom KeyStore PassPhrase, Custom KeyStore Path, Custom KeyStore Type, Custom TrustStore PassPhrase, Custom TrustStore Path.

Verifies that Custom KeyStore Path and Custom TrustStore Path are null or the paths exist.

**Steps Executed**

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



### Steps Used in WebLogic - Provision Weblogic Domain and Admin Server

Workflow Step	Description
Get WebLogic Call-Wrappers	This step creates the commands that subsequent steps will use to execute scripts and WebLogic Scripting Tool (WLST) operations.
Weblogic Domain Admin Server Validate Parameters	This step prepares and validates the parameters needed to create a WebLogic domain and Administration Server.
Create Weblogic Domain Admin Server	This step creates a WebLogic domain and Administration Server. Optionally, the step configures SSL custom keystore and truststore. Optionally, the step enables SSL.
Start Weblogic Node Manager	This step checks if Start Node Manager is set to true. If so, it starts the WebLogic Node Manager process on the target server. Then the step verifies that the Node Manager started.
Start Weblogic Admin Server	This step starts the WebLogic Administration Server.

For parameter descriptions and defaults, see [Parameters for WebLogic - Provision Weblogic Domain and Admin Server](#).

## How to Run this Workflow

The following instructions show you how to customize and run the [WebLogic - Provision Weblogic Domain and Admin Server](#) workflow in your environment.

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

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

**Note:** Before following this procedure, review the [Prerequisites for this Workflow](#) on page 53, and ensure that all requirements are satisfied.

### To use the WebLogic - Provision Weblogic Domain and Admin Server workflow:

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

#### Input Parameters for Get WebLogic Call-Wrappers

Parameter Name	Default Value	Required	Description
BEA Home	no default	required	Fully qualified path to the middleware home directory that contains the WebLogic installation. For example: <code>/opt/oracle/weblogic</code>
WLS Install Home	no default	required	Fully qualified path to the directory where WebLogic Server will be installed. For example: <code>/opt/oracle/weblogic/wlserver12.1</code>

#### Input Parameters for Weblogic Domain Admin Server Validate Parameters

Parameter Name	Default Value	Required	Description
Admin Server Name	no default	required	Label or name given to the Administration Server.
Admin Server Port	no default	required	The non-SSL port on which the WebLogic Administration Server will run.

### Input Parameters for Weblogic Domain Admin Server Validate Parameters, continued

Parameter Name	Default Value	Required	Description
Domain Path	no default	required	Fully qualified path where the domain and domain configuration will be created. For example: <code>/opt/weblogic/user_projects/domains</code>
Enable SSL	false	required	Tells the WebLogic Administration Server to either use (true) or not use (false) the SSL port for communication.
Setup Custom SSL Stores	no default	required	Determines whether you want to run Secure Socket Layer (SSL) with the demo SSL certificates or with your own custom keystore and truststore. Valid values are true or false.  If Setup Custom SSL Stores is true, the following parameters must also be specified: Custom KeyStore PassPhrase, Custom KeyStore Path, Custom KeyStore Type, Custom TrustStore PassPhrase, Custom TrustStore Path, and Private Key Alias.
Start Node Manager	true	required	Determines whether to start the WebLogic Node Manager. Valid values are true and false.
Weblogic Admin Password	no default	required	The password that will be used to authenticate with the WebLogic Administration Server.

**Tip:** To avoid having to re-enter passwords whenever they change, you can create a policy to provide them to the workflow (see [How to Use a Policy to Specify Parameter Values](#) on page 132).

**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 [How to Expose Additional Workflow Parameters](#) on page 131

See [Parameters for WebLogic - Provision Weblogic Domain and Admin Server](#) for detailed descriptions of all input parameters for this workflow, including default values.

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

**Note:** The target for this deployment should be set to the server where the WebLogic Administration Server will be provisioned.

8. Save the deployment (click **Save** in the lower right corner).
9. Run the workflow using this deployment (see "Run Your Workflow" in *HP DMA Quick Start Tutorial* for instructions).

**To verify the results:**

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

*Optional:* If you want to further verify the results:

1. View the {DomainPath}/servers/AdminServer/logs/AdminServer.log file.  
This file is created when the Admin Server is started up.
2. Look for the following to see if the Admin Server started up cleanly:  
Server started in RUNNING mode.

## Sample Scenario

This topic shows you typical parameter values for different use cases for the [WebLogic - Provision Weblogic Domain and Admin Server](#) workflow.

### Scenario 1: Create a Domain and Administration Server without configuring or enabling SSL

Set Setup Custom SSL Stores and Enable SSL to false.

Input Parameters for Get WebLogic Call-Wrappers

Parameter Name	Example Value	Description
BEA Home	see description	Fully qualified path to the middleware home directory that contains the WebLogic installation. For example:  <code>/opt/oracle/weblogic</code>
WLS Install Home	see description	Fully qualified path to the directory where WebLogic Server will be installed. For example:  <code>/opt/oracle/weblogic/wlserver12.1</code>

Input Parameters for Weblogic Domain Admin Server Validate Parameters

Parameter Name	Example Value	Description
Admin Server Name	myAdminServer	Label or name given to the Administration Server.
Admin Server Port	8001	The non-SSL port on which the WebLogic Administration Server will run.
Domain Path	see description	Fully qualified path where the domain and domain configuration will be created. For example:  <code>/opt/weblogic/user_projects/domains</code>
Enable SSL	false	Tells the WebLogic Administration Server to either use (true) or not use (false) the SSL port for communication.
Setup Custom SSL Stores	false	Determines whether you want to run Secure Socket Layer (SSL) with the demo SSL certificates or with your own custom keystore and truststore. Valid values are true or false.  If Setup Custom SSL Stores is true, the following parameters must also be specified: Custom KeyStore PassPhrase, Custom KeyStore Path, Custom KeyStore Type, Custom TrustStore PassPhrase, Custom TrustStore Path, and Private Key Alias.

Input Parameters for Weblogic Domain Admin Server Validate Parameters, continued

Parameter Name	Example Value	Description
Start Node Manager	true	Determines whether to start the WebLogic Node Manager. Valid values are true and false.
Weblogic Admin Password	password	The password that will be used to authenticate with the WebLogic Administration Server.

Be sure that the default values for all remaining input parameters are appropriate for your environment (see [Parameters for WebLogic - Provision Weblogic Domain and Admin Server](#)).

### Scenario 2: Create a Domain and Administration Server and configure and enable SSL

Use this case to set up SSL to have the Node Manager communicate via SSL. Set Setup Custom SSL Stores to true. Also provide values for the following parameters: Custom KeyStore Path, Custom KeyStore PassPhrase, Custom TrustStore Path, Custom TrustStore PassPhrase, and Private Key Alias.

If you want to enable the SSL port for communication set Enable SSL to true and set Admin SSL Port to the port number.

#### Input Parameters for Get WebLogic Call-Wrappers

Parameter Name	Example Value	Description
BEA Home	see description	Fully qualified path to the middleware home directory that contains the WebLogic installation. For example:  /opt/oracle/weblogic
WLS Install Home	see description	Fully qualified path to the directory where WebLogic Server will be installed. For example:  /opt/oracle/weblogic/wlserver12.1

#### Input Parameters for Weblogic Domain Admin Server Validate Parameters

Parameter Name	Example Value	Description
Admin SSL Port	8002	The Secure Sockets Layer (SSL) port on which the WebLogic Administration Server will run. If Enable SSL is set to true, this parameter must also have a value.
Admin Server Name	myAdminServer	Label or name given to the Administration Server.
Admin Server Port	8001	The non-SSL port on which the WebLogic Administration Server will run.
Custom KeyStore PassPhrase	password	Password for the custom keystore.
Custom KeyStore Path	/opt/WebLogic/keystore	Fully qualified path to the custom keystore file.
Custom KeyStore Type	JKS	The type of the Identity keystore.

### Input Parameters for WebLogic Domain Admin Server Validate Parameters, continued

Parameter Name	Example Value	Description
Custom TrustStore PassPhrase	password	Password for the custom truststore.
Custom TrustStore Path	/opt/WebLogic/truststore	Fully qualified path to the custom truststore file.
Domain Path	see description	Fully qualified path where the domain and domain configuration will be created. For example:  /opt/weblogic/user_projects/domains
Enable SSL	true	Tells the WebLogic Administration Server to either use (true) or not use (false) the SSL port for communication.
Private Key Alias	Hostname	The keystore attribute that defines the string alias used to store and retrieve the server's private key.
Setup Custom SSL Stores	true	Determines whether you want to run Secure Socket Layer (SSL) with the demo SSL certificates or with your own custom keystore and truststore. Valid values are true or false.  If Setup Custom SSL Stores is true, the following parameters must also be specified: Custom KeyStore PassPhrase, Custom KeyStore Path, Custom KeyStore Type, Custom TrustStore PassPhrase, Custom TrustStore Path, and Private Key Alias.
Start Node Manager	true	Determines whether to start the WebLogic Node Manager. Valid values are true and false.
Weblogic Admin Password	password	The password that will be used to authenticate with the WebLogic Administration Server.

**Note:** Some of these parameters are not exposed by default in the deployment. See [How to Expose Additional Workflow Parameters](#) on page 131.

You need to expose the following parameters: Admin SSL Port, Custom KeyStore PassPhrase, Custom KeyStore Path, Custom KeyStore Type, Custom TrustStore PassPhrase, and Custom TrustStore Path.

Be sure that the default values for all remaining input parameters are appropriate for your environment (see [Parameters for WebLogic - Provision WebLogic Domain and Admin Server](#)).

## Parameters for WebLogic - Provision Weblogic Domain and Admin Server

The following tables describe the required and optional input parameters for this workflow. Some of these parameters may not be initially visible in a deployment (see [How to Expose Additional Workflow Parameters](#) on page 131). For some parameters, if you do not specify a value for a parameter, a default value is assigned.

Following are tables for each of the steps used by this workflow where parameters are defined:

### Parameters Defined in this Step: Get WebLogic Call-Wrappers

Parameter Name	Default Value	Required	Description
BEA Home	no default	required	Fully qualified path to the middleware home directory that contains the WebLogic installation. For example:  <code>/opt/oracle/weblogic</code>
WLS Install Home	no default	required	Fully qualified path to the directory where WebLogic Server will be installed. For example:  <code>/opt/oracle/weblogic/wlserver12.1</code>

### Additional Parameters Defined in this Step: Weblogic Domain Admin Server Validate Parameters

Parameter Name	Default Value	Required	Description
Admin SSL Port	no default	optional	The Secure Sockets Layer (SSL) port on which the WebLogic Administration Server will run. If Enable SSL is set to true, this parameter must also have a value.
Admin Server Hostname	Server.name	required	The WebLogic Administration Server host name or IP address that the Administration Server will run on. The Administration Server is used to issue administrative commands to the Application Servers.
Admin Server Name	no default	required	Label or name given to the Administration Server.
Admin Server Port	no default	required	The non-SSL port on which the WebLogic Administration Server will run.

Additional Parameters Defined in this Step: Weblogic Domain Admin Server Validate Parameters, continued

Parameter Name	Default Value	Required	Description
Call Wrapper	see description	required	<p>Command that will execute this step (or subsequent steps) as a specific user.</p> <p>For UNIX targets, the default is: /opt/hp/dma/client/jython.sh running as root</p> <p>For Windows targets, the default is: jython running as Administrator</p> <p><b>Caution:</b> This parameter is derived by the workflow. Under most circumstances, you should not change its mapping or its value.</p>
Custom KeyStore PassPhrase	no default	optional	Password for the custom keystore.
Custom KeyStore Path	no default	optional	Fully qualified path to the custom keystore file.
Custom KeyStore Type	JKS	optional	The type of the Identity keystore.
Custom TrustStore PassPhrase	no default	optional	Password for the custom truststore.
Custom TrustStore Path	no default	optional	Fully qualified path to the custom truststore file.
Domain Path	no default	required	<p>Fully qualified path where the domain and domain configuration will be created. For example:</p> <p>/opt/weblogic/user_projects/domains</p>
Enable SSL	false	required	Tells the WebLogic Administration Server to either use (true) or not use (false) the SSL port for communication.
Node Manager Port	5556	optional	Sets the port number under which the Node Manager will run.
Private Key Alias	no default	optional	The keystore attribute that defines the string alias used to store and retrieve the server's private key.

Additional Parameters Defined in this Step: Weblogic Domain Admin Server Validate Parameters, continued

Parameter Name	Default Value	Required	Description
Setup Custom SSL Stores	no default	required	<p>Determines whether you want to run Secure Socket Layer (SSL) with the demo SSL certificates or with your own custom keystore and truststore. Valid values are true or false.</p> <p>If Setup Custom SSL Stores is true, the following parameters must also be specified: Custom KeyStore PassPhrase, Custom KeyStore Path, Custom KeyStore Type, Custom TrustStore PassPhrase, Custom TrustStore Path, and Private Key Alias.</p>
Start Node Manager	true	required	Determines whether to start the WebLogic Node Manager. Valid values are true and false.
WLST Call Wrapper	no default	required	<p>Command that will invoke the WebLogic Scripting Tool (WLST). For example:</p> <pre>su &lt;user&gt; /opt/oracle/WebLogic/install/common/bin/wlst.sh</pre> <p>The fully qualified path will vary depending on where you installed the product. The &lt;user&gt; must have appropriate permissions.</p> <div> <p><b>Caution:</b> This parameter is derived by the workflow. Under most circumstances, you should not change its mapping or its value.</p> </div>
Weblogic Admin Password	no default	required	The password that will be used to authenticate with the WebLogic Administration Server.

# WebLogic - Provision Advanced Domain and Admin Server

This workflow modifies an existing WebLogic domain and Administration Server, enables the domain-wide administration port, configures logging attributes of the domain and Administration Server, and modifies the WebLogic Scripting Tool (WLST) script to enable connection through the WLST to the domain-wide administration port.

## Benefits

This workflow has the following benefits:

- You need to have SSL configured before you run the workflow to enable the domain-wide administration port.
- The domain-wide administration port changes the behavior of the traffic between the Administration Server and the application servers.
- You can put the application servers into stand-by mode, allowing a hot swap.
- The workflow changes the WLST script to configure SSL communication to the domain-wide administration port.

For information about how this workflow can be used with other WebLogic provisioning workflows see [How to Use the Workflows Together](#) on page 19.

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

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

## Prerequisites for this Workflow

Be sure that the following prerequisites are satisfied before you run the [WebLogic - Provision Advanced Domain and Admin Server](#) workflow:

1. The latest HP DMA solution packs require the latest HP DMA platform. To use the latest solution packs, update the HP DMA platform. HP DMA 10.30 solution packs are supported on HP DMA 10.30 (and later).
2. You have installed the Application Server Provisioning Solution Pack.
3. The WebLogic domain and Administration Server must exist and be configured to use SSL.

For more information about prerequisites for WebLogic 11g and 12c, refer to the [WebLogic Product Documentation](#) on page 125.

## How this Workflow Works

The following information describes how the [WebLogic - Provision Advanced Domain and Admin Server](#) workflow works:

### Overview

The workflow does the following:

- Prepares to modify the WebLogic domain and Administration Server advanced configurations by setting up the command to be used in subsequent steps, gathering and validating input parameters, and validating connection to the Administration Server.
- Uses the existing SSL keystore and truststore configurations and components that were previously created by the [WebLogic - Create Trust and Identity Keystore](#).
- Modifies an existing WebLogic domain and Administration Server—created by [WebLogic - Provision Weblogic Domain and Admin Server](#)—to enable the domain-wide administration port and configure logging attributes.
- Modifies the WLST script to enable connection through WLST to the domain-wide administration port.
- Stops and restarts the WebLogic Administration Server so that the changes take affect and then validates that the Administration Server came up successfully.

### Validation Checks Performed

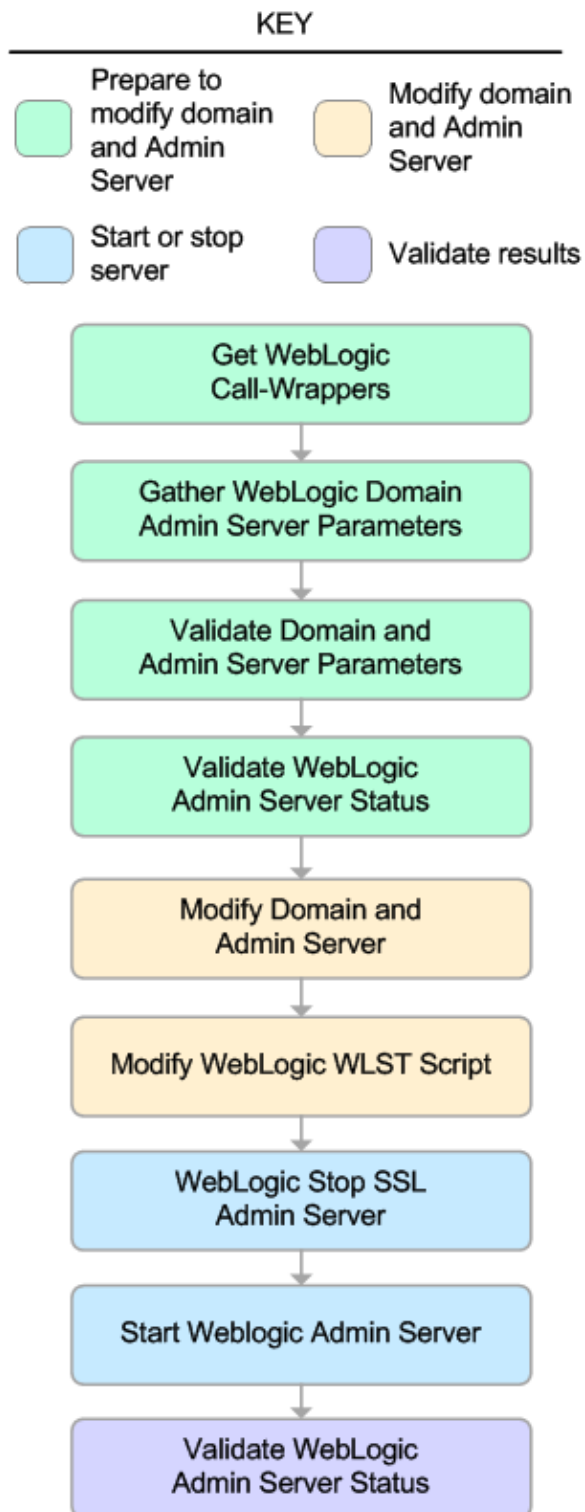
Much of the validation centers on the input parameters:

- Verifies that required parameters have values specified.
- Verifies that Admin Server Log Dir, Domain Path, Java Home,, and WLS Install Home are valid paths and exist.
- Verifies that TrustStore File Locations a valid existing path with a valid filename.
- Verifies that Admin Server Port, Admin SSL Port, and Domain Administration Port are valid integers.

The workflow also validates that the Administration Server is up and running before and after making the modifications.

### Steps Executed

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



### Steps Used in WebLogic - Provision Advanced Domain and Admin Server

Workflow Step	Description
Get WebLogic Call-Wrappers	This step creates the commands that subsequent steps will use to execute scripts and WebLogic Scripting Tool (WLST) operations.
Gather WebLogic Domain Admin Server Parameters	This step gathers all required parameters to enable the domain-wide administration port, modify logging attributes, and modify the WLST script file.
Validate Domain and Admin Server Parameters	This step validates and prepares all required parameters to enable the domain-wide administration port, modify logging attributes, and modify the WLST script file.
Validate WebLogic Admin Server Status	This step validates that the Administration Server process is up and running.
Modify Domain and Admin Server	This step enables the domain-wide administration port and modifies logging attributes for the Administration Server.
Modify WebLogic WLST Script	This step modifies the WLST script file on the target machine to enable connections to the domain-wide administration port.
WebLogic Stop SSL Admin Server	This step stops the Administration SSL Server on a given machine or server.
Start Weblogic Admin Server	This step starts the WebLogic Administration Server.
Validate WebLogic Admin Server Status	This step validates that the Administration Server process is up and running.

For parameter descriptions and defaults, see [Parameters for WebLogic - Provision Advanced Domain and Admin Server](#).

## How to Run this Workflow

The following instructions show you how to customize and run the [WebLogic - Provision Advanced Domain and Admin Server](#) workflow in your environment.

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

**Note:** Before following this procedure, review the [Prerequisites for this Workflow](#) on page 68, and ensure that all requirements are satisfied.

### To use the WebLogic - Provision Weblogic Domain and Admin Server workflow:

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

#### Input Parameters for Get WebLogic Call-Wrappers

Parameter Name	Default Value	Required	Description
BEA Home	no default	required	Fully qualified path to the middleware home directory that contains the WebLogic installation. For example: <code>/opt/oracle/weblogic</code>
WLS Install Home	no default	required	Fully qualified path to the directory where WebLogic Server will be installed. For example: <code>/opt/oracle/weblogic/wlserver12.1</code>

#### Input Parameters for Gather WebLogic Domain Admin Server Parameters

Parameter Name	Default Value	Required	Description
Admin SSL Port	no default	required	The Secure Sockets Layer (SSL) port on which the WebLogic Administration Server will run. If Enable SSL is set to true, this parameter must also have a value.
Admin Server Hostname	Server.name	required	The WebLogic Administration Server host name or IP address that the Administration Server will run on. The Administration Server is used to issue administrative commands to the Application Servers.
Admin Server Log Dir	no default	required	Log file directory location where the Administration Server logs will be written.

### Input Parameters for Gather WebLogic Domain Admin Server Parameters, continued

Parameter Name	Default Value	Required	Description
Admin Server Name	no default	required	Label or name given to the Administration Server.
Admin Server Port	no default	required	The non-SSL port on which the WebLogic Administration Server will run.
Domain Administration Port	no default	required	The common secure administration port for this WebLogic Server domain.
Domain Name	no default	required	Name of the WebLogic Server domain.
Domain Path	no default	required	Fully qualified path where the domain and domain configuration will be created. For example: <code>/opt/weblogic/user_projects/domains</code>
Java Home	no default	required	Fully qualified path to the JAVA_HOME that the WebLogic domain uses. For example: <code>/opt/oracle/jdk1.6.0_35</code>
TrustStore File Location	no default	required	Fully qualified file path where the java truststore already exists. For example: <code>/opt/app/ssl/mytruststore.jks</code>
Weblogic Admin Password	no default	required	The password that will be used to authenticate with the WebLogic Administration Server.
WebLogic Admin User	no default	required	The WebLogic administrator account that will be used to authenticate with the Administration Server.

**Tip:** To avoid having to re-enter passwords whenever they change, you can create a policy to provide them to the workflow (see [How to Use a Policy to Specify Parameter Values](#) on page 132).

**Note:** See [Parameters for WebLogic - Provision Advanced Domain and Admin Server](#) for detailed descriptions of all input parameters for this workflow, including default values.

3. In the workflow editor, expose any additional parameters that you need. You will specify values for those parameters when you create the deployment.
4. Save the changes to the workflow (click **Save** in the lower right corner).
5. Create a new deployment (see "Create a Deployment" in *HP DMA Quick Start Tutorial* for instructions).
6. On the Parameters tab, specify values for the required parameters listed in step 2 and any

additional parameters that you have exposed. You do not need to specify values for those parameters whose default values are appropriate for your environment.

7. On the Targets tab, specify one or more targets for this deployment.

**Note:** The target for this deployment should be set to the server where the WebLogic Administration Server will be provisioned.

8. Save the deployment (click **Save** in the lower right corner).
9. Run the workflow using this deployment (see "Run Your Workflow" in *HP DMA Quick Start Tutorial* for instructions).

**To verify the results:**

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

*Optional:* If you want to further verify the results:

The workflow was successful if the Administration Server restarted successfully.

## Sample Scenario

It is very straightforward to run the [WebLogic - Provision Advanced Domain and Admin Server](#) workflow. This topic shows you typical parameter values to use.

### Typical parameters

#### Input Parameters for Get WebLogic Call-Wrappers

Parameter Name	Example Value	Description
BEA Home	see description	Fully qualified path to the middleware home directory that contains the WebLogic installation. For example:  <code>/opt/oracle/weblogic</code>
WLS Install Home	see description	Fully qualified path to the directory where WebLogic Server will be installed. For example:  <code>/opt/oracle/weblogic/wlserver12.1</code>

#### Input Parameters for Gather WebLogic Domain Admin Server Parameters

Parameter Name	Example Value	Description
Admin SSL Port	8002	The Secure Sockets Layer (SSL) port on which the WebLogic Administration Server will run. If Enable SSL is set to true, this parameter must also have a value.
Admin Server Log Dir	<code>/opt/oracle/weblogic/logs/admin.log</code>	Log file directory location where the Administration Server logs will be written.
Admin Server Name	myAdminServer	Label or name given to the Administration Server.
Admin Server Port	8001	The non-SSL port on which the WebLogic Administration Server will run.
Domain Administration Port	5555	The common secure administration port for this WebLogic Server domain.
Domain Name	MyDomain	Name of the WebLogic Server domain.
Domain Path	see description	Fully qualified path where the domain and domain configuration will be created. For example:  <code>/opt/weblogic/user_projects/domains</code>
Java Home	see description	Fully qualified path to the JAVA_HOME that the WebLogic domain uses.  For example: <code>/opt/oracle/jdk1.6.0_35</code>

Input Parameters for Gather WebLogic Domain Admin Server Parameters, continued

Parameter Name	Example Value	Description
TrustStore File Location	see description	Fully qualified file path where the java truststore already exists.  For example: /opt/app/ssl/mytruststore.jks
Weblogic Admin Password	password	The password that will be used to authenticate with the WebLogic Administration Server.
WebLogic Admin User	weblogic	The WebLogic administrator account that will be used to authenticate with the Administration Server.

## Parameters for WebLogic - Provision Advanced Domain and Admin Server

The following tables describe the required and optional input parameters for this workflow. Some of these parameters may not be initially visible in a deployment (see [How to Expose Additional Workflow Parameters](#) on page 131). For some parameters, if you do not specify a value for a parameter, a default value is assigned.

Following are tables for each of the steps used by this workflow where parameters are defined:

### Parameters Defined in this Step: Get WebLogic Call-Wrappers

Parameter Name	Default Value	Required	Description
BEA Home	no default	required	Fully qualified path to the middleware home directory that contains the WebLogic installation. For example:  <code>/opt/oracle/weblogic</code>
WLS Install Home	no default	required	Fully qualified path to the directory where WebLogic Server will be installed. For example:  <code>/opt/oracle/weblogic/wlserver12.1</code>

### Additional Parameters Defined in this Step: Gather WebLogic Domain Admin Server Parameters

Parameter Name	Default Value	Required	Description
Admin SSL Port	no default	required	The Secure Sockets Layer (SSL) port on which the WebLogic Administration Server will run. If Enable SSL is set to true, this parameter must also have a value.
Admin Server Hostname	Server.name	required	The WebLogic Administration Server host name or IP address that the Administration Server will run on. The Administration Server is used to issue administrative commands to the Application Servers.
Admin Server Log Dir	no default	required	Log file directory location where the Administration Server logs will be written.
Admin Server Name	no default	required	Label or name given to the Administration Server.
Admin Server Port	no default	required	The non-SSL port on which the WebLogic Administration Server will run.
Domain Administration Port	no default	required	The common secure administration port for this WebLogic Server domain.
Domain Name	no default	required	Name of the WebLogic Server domain.

Additional Parameters Defined in this Step: Gather WebLogic Domain Admin Server Parameters, continued

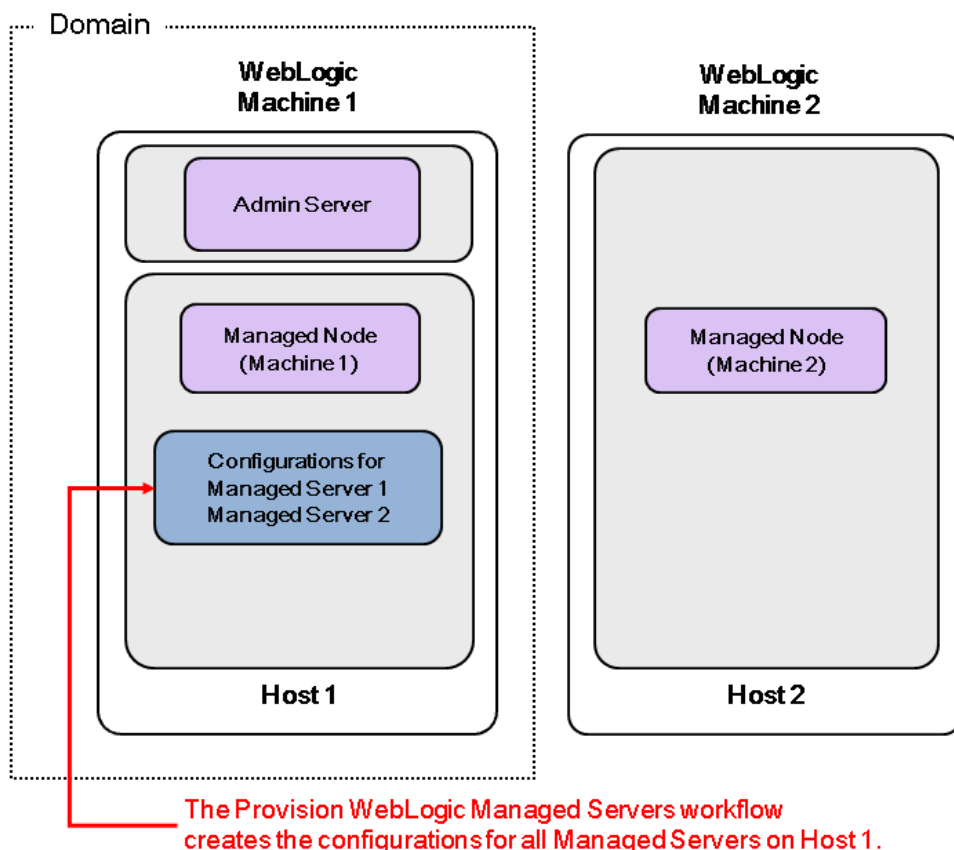
Parameter Name	Default Value	Required	Description
Domain Path	no default	required	Fully qualified path where the domain and domain configuration will be created. For example:  /opt/weblogic/user_projects/domains
Java Home	no default	required	Fully qualified path to the JAVA_HOME that the WebLogic domain uses.  For example: /opt/oracle/jdk1.6.0_35
TrustStore File Location	no default	required	Fully qualified file path where the java truststore already exists.  For example: /opt/app/ssl/mytruststore.jks
Weblogic Admin Password	no default	required	The password that will be used to authenticate with the WebLogic Administration Server.
WebLogic Admin User	no default	required	The WebLogic administrator account that will be used to authenticate with the Administration Server.

## WebLogic - Provision Weblogic Managed Servers

This workflow creates a configuration for a WebLogic Managed Server (or servers) from an existing installation and domain of WebLogic.

You can group application servers together to optimize availability and scalability, or to manage your workload.

The following reference architecture diagram gives an example of what this workflow does:



For information about how this workflow can be used with other WebLogic provisioning workflows see [How to Use the Workflows Together](#) on page 19.

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

Topic	Information Included
<a href="#">Prerequisites for this Workflow</a>	List of prerequisites that must be satisfied before you can run this workflow
<a href="#">How this Workflow Works</a>	Information about what the workflow does, including validation checks performed, steps executed, and a high-level process flow
<a href="#">How to Run this Workflow</a>	Instructions for running this workflow in your environment
<a href="#">Sample Scenario</a>	Examples of typical parameter values for this workflow
<a href="#">Parameters</a>	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 HP DMA user interface may have a version appended, for example, v2.

## Prerequisites for this Workflow

Be sure that the following prerequisites are satisfied before you run the [WebLogic - Provision Weblogic Managed Servers](#) workflow:

1. The latest HP DMA solution packs require the latest HP DMA platform. To use the latest solution packs, update the HP DMA platform. HP DMA 10.30 solution packs are supported on HP DMA 10.30 (and later).
2. You have installed the Application Server Provisioning Solution Pack.

For more information about prerequisites for WebLogic 11g and 12c, refer to the [WebLogic Product Documentation](#) on page 125.

## How this Workflow Works

The following information describes how the [WebLogic - Provision Weblogic Managed Servers](#) workflow works:

### Overview

The workflow does the following:

- Prepares to provision the WebLogic Managed Servers by setting up the command to be used in subsequent steps and validating input parameters.
- Creates the configurations for the Managed Servers using the WebLogic Scripting Tool (WLST). To do this, the workflow accesses the domain information, creates the servers, and then updates the domain.
- Stops and restarts the WebLogic Administration Server and then starts any Managed Servers.

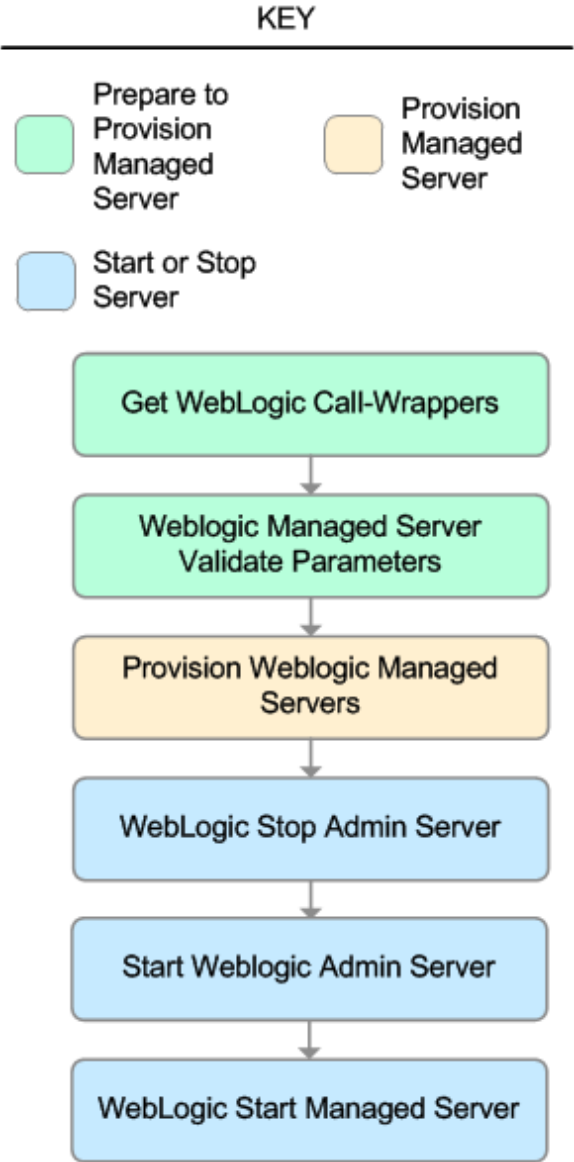
### Validation Checks Performed

Much of the validation centers on the input parameters:

- Verifies that required parameters have values specified.
- Checks that the BEA Home and WLS Install Home files exist.
- Verifies that Enable Managed Server SSL, Setup Server Custom SSL, and Start Managed Servers are either true or false.
- If Setup Server Custom SSL is true, then Custom KeyStore PassPhrase, Custom KeyStore Path, Custom TrustStore PassPhrase, Custom TrustStore Path, and Private Key Alias are specified.
- Verifies that Managed Server Ports, Managed Server SSL Ports, and Managed Server Admin Ports are null or valid integers.
- Verifies that the lists are the same length for Managed Server Hostnames, Managed Server Names, Managed Server Ports, and Managed Server SSL Ports.

**Steps Executed**

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



### Steps Used in WebLogic - Provision Weblogic Managed Servers

Workflow Step	Description
Get WebLogic Call-Wrappers	This step creates the commands that subsequent steps will use to execute scripts and WebLogic Scripting Tool (WLST) operations.
Weblogic Managed Server Validate Parameters	This step prepares the parameters needed to create a Managed Server in WebLogic.
Provision Weblogic Managed Servers	This step creates Managed Servers from an existing domain in WebLogic. Optionally, the step enables SSL for the Managed Servers and configures the SSL port to listen. Optionally, the step configures the custom keystore and truststore. Optionally, if the <a href="#">WebLogic - Provision Advanced Domain and Admin Server</a> was run before this workflow, the step sets up the optional Domain Administration Port.
WebLogic Stop Admin Server	This step checks if the WebLogic Administration Server on a given machine or server is running. If it is running, the step stops it.
Start Weblogic Admin Server	This step starts the WebLogic Administration Server.
WebLogic Start Managed Server	This step connects to WebLogic via WebLogic Scripting Tool (WLST) and optionally starts all Managed Servers on a given machine or server.

For parameter descriptions and defaults, see [Parameters for WebLogic - Provision Weblogic Managed Servers](#).

## How to Run this Workflow

The following instructions show you how to customize and run the [WebLogic - Provision Weblogic Managed Servers](#) workflow in your environment.

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

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

**Note:** Before following this procedure, review the [Prerequisites for this Workflow](#) on page 81, and ensure that all requirements are satisfied.

### To use the WebLogic - Provision Weblogic Managed Servers workflow:

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

#### Input Parameters for Get WebLogic Call-Wrappers

Parameter Name	Default Value	Required	Description
BEA Home	no default	required	Fully qualified path to the middleware home directory that contains the WebLogic installation. For example: <code>/opt/oracle/weblogic</code>
WLS Install Home	no default	required	Fully qualified path to the directory where WebLogic Server will be installed. For example: <code>/opt/oracle/weblogic/wlserver12.1</code>

#### Input Parameters for Weblogic Managed Server Validate Parameters

Parameter Name	Default Value	Required	Description
Admin Server Name	no default	required	Label or name given to the Administration Server.
Admin Server Port	no default	required	The non-SSL port on which the WebLogic Administration Server will run.
Custom KeyStore PassPhrase	no default	optional	Password for the custom keystore.

Input Parameters for Weblogic Managed Server Validate Parameters, continued

Parameter Name	Default Value	Required	Description
Custom KeyStore Path	no default	optional	Fully qualified path to the custom keystore file.
Custom TrustStore PassPhrase	no default	optional	Password for the custom truststore.
Custom TrustStore Path	no default	optional	Fully qualified path to the custom truststore file.
Domain Administration Port	no default	required	The common secure administration port for this WebLogic Server domain.
Domain Path	no default	required	Fully qualified path where the domain and domain configuration will be created. For example: <code>/opt/weblogic/user_projects/domains</code>
Enable Managed Server SSL	no default	required	This parameter determines whether the Managed Server will use or not use the Secure Sockets Layer (SSL) port for communication. Valid values are true or false.
Managed Server Admin Ports	no default	required	The common secure domain-wide administration port that the Administration Server and Managed Server will communicate on.
Managed Server Hostnames	no default	required	Comma-delimited list of host names or IP addresses where each Managed Server will be provisioned.  <b>Note:</b> The order of the host names or IP addresses specified must match the order specified in the following parameters: Managed Server Names, Managed Server Ports, and Managed Server SSL Ports.

Input Parameters for Weblogic Managed Server Validate Parameters, continued

Parameter Name	Default Value	Required	Description
Managed Server Names	no default	required	<p>Comma-delimited list of the names of the Managed Servers to be provisioned. For example: Appserver1, Appserver2, Appserver3.</p> <p><b>Note:</b> The order of the server names specified must match the order specified in the following parameters: Managed Server Hostnames, Managed Server Ports, and Managed Server SSL Ports.</p>
Managed Server Ports	no default	required	<p>Comma-delimited list of the ports on which the Managed Servers will listen.</p> <p><b>Note:</b> The order of the ports specified must match the order specified in the following parameters: Managed Server Hostnames, Managed Server Names, and Managed Server SSL Ports.</p>
Managed Server SSL Ports	no default	optional	<p>Comma-delimited list of SSL ports on which the Managed Servers will listen.</p> <p><b>Note:</b> The order of the SSL ports specified must match the order specified in the following parameters: Managed Server Hostnames, Managed Server Names, and Managed Server Ports.</p>
Private Key Alias	no default	optional	<p>The keystore attribute that defines the string alias used to store and retrieve the server's private key.</p>
Setup Server Custom SSL Stores	no default	required	<p>Determines whether you want to run Secure Socket Layer (SSL) with the demo SSL certificates or with your own custom keystore and truststore. Valid values are true or false.</p> <p>If Setup Server Custom SSL Stores is true, the following parameters must also be specified: Custom KeyStore Path, Custom KeyStore PassPhrase, Custom TrustStore Path, Custom TrustStore PassPhrase, and Private Key Alias.</p>
Start Managed Servers	true	optional	<p>Specifies whether or not to start up the managed servers once they have been created. Valid values are true and false.</p>

#### Input Parameters for Weblogic Managed Server Validate Parameters, continued

Parameter Name	Default Value	Required	Description
WebLogic User Id	no default	required	The WebLogic user that will be used to authenticate with the Administration Server.
WebLogic User Password	no default	required	The WebLogic password that will be used to authenticate with the Administration Server.

**Tip:** To avoid having to re-enter passwords whenever they change, you can create a policy to provide them to the workflow (see [How to Use a Policy to Specify Parameter Values](#) on page 132).

**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 [How to Expose Additional Workflow Parameters](#) on page 131

See [Parameters for WebLogic - Provision Weblogic Managed Servers](#) for detailed descriptions of all input parameters for this workflow, including default values.

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

**Note:** The target for this deployment should be set to the server where the WebLogic Administration Server is provisioned.

8. Save the deployment (click **Save** in the lower right corner).
9. Run the workflow using this deployment (see "Run Your Workflow" in *HP DMA Quick Start Tutorial* for instructions).

#### To verify the results:

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

*Optional:* If you want to further verify the results:

1. View the `{DomainPath}/servers/{ManagedServerName}/logs/{ManagedServerName}.log` file.  
This file is created when the Managed Server is started up.

2. Look for the following to verify that the Managed Server (or servers) started:  
Server started in RUNNING mode.

## Sample Scenario

This topic shows you typical parameter values for different use cases for the [WebLogic - Provision Weblogic Managed Servers](#) workflow.

### Scenario 1: Creates three Managed Servers on three separate hosts without configuring or enabling SSL

Set Setup Custom SSL Stores to false. Do not provide values for the following parameters: Custom KeyStore Path, Custom KeyStore PassPhrase, Custom TrustStore Path, Custom TrustStore PassPhrase, and Private Key Alias.

This scenario creates the following configuration of Managed Servers:

#### Managed Server configuration

Managed Server Name	Managed Server Hostname	Managed Server Port
Appserver1	Host1	8001
Appserver2	Host2	8002
Appserver3	Host3	8003

#### Input Parameters for Get WebLogic Call-Wrappers

Parameter Name	Example Value	Description
BEA Home	see description	Fully qualified path to the middleware home directory that contains the WebLogic installation. For example:  /opt/oracle/weblogic
WLS Install Home	see description	Fully qualified path to the directory where WebLogic Server will be installed. For example:  /opt/oracle/weblogic/wlserver12.1

#### Input Parameters for Weblogic Managed Server Validate Parameters

Parameter Name	Example Value	Description
Admin Server Name	myAdminServer	Label or name given to the Administration Server.
Admin Server Port	8005	The non-SSL port on which the WebLogic Administration Server will run.
Custom KeyStore PassPhrase		Password for the custom keystore.

### Input Parameters for Weblogic Managed Server Validate Parameters, continued

Parameter Name	Example Value	Description
Custom KeyStore Path		Fully qualified path to the custom keystore file.
Custom TrustStore PassPhrase		Password for the custom truststore.
Custom TrustStore Path		Fully qualified path to the custom truststore file.
Domain Administration Port	5555	The common secure administration port for this WebLogic Server domain.
Domain Path	see description	Fully qualified path where the domain and domain configuration will be created. For example:  <code>/opt/weblogic/user_projects/domains</code>
Enable Managed Server SSL	false	This parameter determines whether the Managed Server will use or not use the Secure Sockets Layer (SSL) port for communication. Valid values are true or false.
Managed Server Admin Ports	5556	The common secure domain-wide administration port that the Administration Server and Managed Server will communicate on.
Managed Server Hostnames	Host1, Host2, Host3	Comma-delimited list of host names or IP addresses where each Managed Server will be provisioned.  <b>Note:</b> The order of the host names or IP addresses specified must match the order specified in the following parameters: Managed Server Names, Managed Server Ports, and Managed Server SSL Ports.
Managed Server Names	AppServer1, AppServer2, AppServer3	Comma-delimited list of the names of the Managed Servers to be provisioned. For example: Appserver1, Appserver2, Appserver3.  <b>Note:</b> The order of the server names specified must match the order specified in the following parameters: Managed Server Hostnames, Managed Server Ports, and Managed Server SSL Ports.

### Input Parameters for WebLogic Managed Server Validate Parameters, continued

Parameter Name	Example Value	Description
Managed Server Ports	8001, 8002, 8003	Comma-delimited list of the ports on which the Managed Servers will listen.  <b>Note:</b> The order of the ports specified must match the order specified in the following parameters: Managed Server Hostnames, Managed Server Names, and Managed Server SSL Ports.
Managed Server SSL Ports		Comma-delimited list of SSL ports on which the Managed Servers will listen.  <b>Note:</b> The order of the SSL ports specified must match the order specified in the following parameters: Managed Server Hostnames, Managed Server Names, and Managed Server Ports.
Setup Server Custom SSL Stores	false	Determines whether you want to run Secure Socket Layer (SSL) with the demo SSL certificates or with your own custom keystore and truststore. Valid values are true or false.  If Setup Server Custom SSL Stores is true, the following parameters must also be specified: Custom KeyStore Path, Custom KeyStore PassPhrase, Custom TrustStore Path, Custom TrustStore PassPhrase, and Private Key Alias.
Start Managed Servers	true	Specifies whether or not to start up the managed servers once they have been created. Valid values are true and false.
WebLogic User Id	weblogic01	The WebLogic user that will be used to authenticate with the Administration Server.
WebLogic User Password	weblogic01	The WebLogic password that will be used to authenticate with the Administration Server.

Be sure that the default values for all remaining input parameters are appropriate for your environment (see [Parameters for WebLogic - Provision Weblogic Managed Servers](#)).

### Scenario 2: Create four Managed Servers on two hosts and configure and enable SSL

Use this case to set up SSL to have the Node Manager communicate via SSL. Set Setup Custom SSL Stores to true. Also provide values for the following parameters: Custom KeyStore Path, Custom KeyStore PassPhrase, Custom TrustStore Path, Custom TrustStore PassPhrase, and Private Key Alias.

This scenario creates the following configuration of Managed Servers:

#### Managed Server configuration

Managed Server Name	Managed Server Hostname	Managed Server Port	Managed Server SSL Port
Appserver1	Host1	8001	8881
Appserver2	Host1	8002	8882
Appserver3	Host2	8001	8881
Appserver4	Host2	8002	8882

#### Input Parameters for Get WebLogic Call-Wrappers

Parameter Name	Example Value	Description
BEA Home	see description	Fully qualified path to the middleware home directory that contains the WebLogic installation. For example:  /opt/oracle/weblogic
WLS Install Home	see description	Fully qualified path to the directory where WebLogic Server will be installed. For example:  /opt/oracle/weblogic/wlserver12.1

#### Input Parameters for Weblogic Managed Server Validate Parameters

Parameter Name	Example Value	Description
Admin Server Name	myAdminServer	Label or name given to the Administration Server.
Admin Server Port	8005	The non-SSL port on which the WebLogic Administration Server will run.
Custom KeyStore PassPhrase	password	Password for the custom keystore.
Custom KeyStore Path	/opt/WebLogic/keystore	Fully qualified path to the custom keystore file.

Input Parameters for WebLogic Managed Server Validate Parameters, continued

Parameter Name	Example Value	Description
Custom TrustStore PassPhrase	password	Password for the custom truststore.
Custom TrustStore Path	/opt/WebLogic/truststore	Fully qualified path to the custom truststore file.
Domain Administration Port	5555	The common secure administration port for this WebLogic Server domain.
Domain Path	see description	Fully qualified path where the domain and domain configuration will be created. For example:  /opt/weblogic/user_projects/domains
Enable Managed Server SSL	true	This parameter determines whether the Managed Server will use or not use the Secure Sockets Layer (SSL) port for communication. Valid values are true or false.
Managed Server Admin Ports	5556	The common secure domain-wide administration port that the Administration Server and Managed Server will communicate on.
Managed Server Hostnames	Host1, Host2, Host1, Host2	Comma-delimited list of host names or IP addresses where each Managed Server will be provisioned.  <b>Note:</b> The order of the host names or IP addresses specified must match the order specified in the following parameters: Managed Server Names, Managed Server Ports, and Managed Server SSL Ports.
Managed Server Names	Appserver1, Appserver2, Appserver3, Appserver4	Comma-delimited list of the names of the Managed Servers to be provisioned. For example: Appserver1, Appserver2, Appserver3.  <b>Note:</b> The order of the server names specified must match the order specified in the following parameters: Managed Server Hostnames, Managed Server Ports, and Managed Server SSL Ports.

### Input Parameters for WebLogic Managed Server Validate Parameters, continued

Parameter Name	Example Value	Description
Managed Server Ports	8001, 8002, 8001, 8002	Comma-delimited list of the ports on which the Managed Servers will listen.  <b>Note:</b> The order of the ports specified must match the order specified in the following parameters: Managed Server Hostnames, Managed Server Names, and Managed Server SSL Ports.
Managed Server SSL Ports	8881,8882,8881, 8882	Comma-delimited list of SSL ports on which the Managed Servers will listen.  <b>Note:</b> The order of the SSL ports specified must match the order specified in the following parameters: Managed Server Hostnames, Managed Server Names, and Managed Server Ports.
Private Key Alias	Hostname	The keystore attribute that defines the string alias used to store and retrieve the server's private key.
Setup Server Custom SSL Stores	true	Determines whether you want to run Secure Socket Layer (SSL) with the demo SSL certificates or with your own custom keystore and truststore. Valid values are true or false.  If Setup Server Custom SSL Stores is true, the following parameters must also be specified: Custom KeyStore Path, Custom KeyStore PassPhrase, Custom TrustStore Path, Custom TrustStore PassPhrase, and Private Key Alias.
Start Managed Servers	true	Specifies whether or not to start up the managed servers once they have been created. Valid values are true and false.
WebLogic User Id	weblogic01	The WebLogic user that will be used to authenticate with the Administration Server.
WebLogic User Password	weblogic01	The WebLogic password that will be used to authenticate with the Administration Server.

Be sure that the default values for all remaining input parameters are appropriate for your environment (see [Parameters for WebLogic - Provision Weblogic Managed Servers](#)).

## Parameters for WebLogic - Provision Weblogic Managed Servers

The following tables describe the required and optional input parameters for this workflow. Some of these parameters may not be initially visible in a deployment (see [How to Expose Additional Workflow Parameters](#) on page 131). For some parameters, if you do not specify a value for a parameter, a default value is assigned.

Following are tables for each of the steps used by this workflow where parameters are defined:

### Parameters Defined in this Step: Get WebLogic Call-Wrappers

Parameter Name	Default Value	Required	Description
BEA Home	no default	required	Fully qualified path to the middleware home directory that contains the WebLogic installation. For example:  <code>/opt/oracle/weblogic</code>
WLS Install Home	no default	required	Fully qualified path to the directory where WebLogic Server will be installed. For example:  <code>/opt/oracle/weblogic/wlserver12.1</code>

### Additional Parameters Defined in this Step: Weblogic Managed Server Validate Parameters

Parameter Name	Default Value	Required	Description
Admin Server Hostname	Server.name	required	The WebLogic Administration Server host name or IP address that the Administration Server will run on. The Administration Server is used to issue administrative commands to the Application Servers.
Admin Server Name	no default	required	Label or name given to the Administration Server.
Admin Server Port	no default	required	The non-SSL port on which the WebLogic Administration Server will run.
Call Wrapper	see description	optional	Command that will execute this step (or subsequent steps) as a specific user.  For UNIX targets, the default is: <code>/opt/hp/dma/client/jython.sh</code> running as root  For Windows targets, the default is: <code>jython</code> running as Administrator  <b>Caution:</b> This parameter is derived by the workflow. Under most circumstances, you should not change its mapping or its value.

Additional Parameters Defined in this Step: Weblogic Managed Server Validate Parameters, continued

Parameter Name	Default Value	Required	Description
Custom KeyStore PassPhrase	no default	optional	Password for the custom keystore.
Custom KeyStore Path	no default	optional	Fully qualified path to the custom keystore file.
Custom TrustStore PassPhrase	no default	optional	Password for the custom truststore.
Custom TrustStore Path	no default	optional	Fully qualified path to the custom truststore file.
Domain Administration Port	no default	required	The common secure administration port for this WebLogic Server domain.
Domain Path	no default	required	Fully qualified path where the domain and domain configuration will be created. For example: <code>/opt/weblogic/user_projects/domains</code>
Enable Managed Server SSL	no default	required	This parameter determines whether the Managed Server will use or not use the Secure Sockets Layer (SSL) port for communication. Valid values are true or false.
Managed Server Admin Ports	no default	required	The common secure domain-wide administration port that the Administration Server and Managed Server will communicate on.
Managed Server Hostnames	no default	required	Comma-delimited list of host names or IP addresses where each Managed Server will be provisioned.  <b>Note:</b> The order of the host names or IP addresses specified must match the order specified in the following parameters: Managed Server Names, Managed Server Ports, and Managed Server SSL Ports.

Additional Parameters Defined in this Step: Weblogic Managed Server Validate Parameters, continued

Parameter Name	Default Value	Required	Description
Managed Server Names	no default	required	<p>Comma-delimited list of the names of the Managed Servers to be provisioned. For example: Appserver1, Appserver2, Appserver3.</p> <p><b>Note:</b> The order of the server names specified must match the order specified in the following parameters: Managed Server Hostnames, Managed Server Ports, and Managed Server SSL Ports.</p>
Managed Server Ports	no default	required	<p>Comma-delimited list of the ports on which the Managed Servers will listen.</p> <p><b>Note:</b> The order of the ports specified must match the order specified in the following parameters: Managed Server Hostnames, Managed Server Names, and Managed Server SSL Ports.</p>
Managed Server SSL Ports	no default	optional	<p>Comma-delimited list of SSL ports on which the Managed Servers will listen.</p> <p><b>Note:</b> The order of the SSL ports specified must match the order specified in the following parameters: Managed Server Hostnames, Managed Server Names, and Managed Server Ports.</p>
Private Key Alias	no default	optional	The keystore attribute that defines the string alias used to store and retrieve the server's private key.
Setup Server Custom SSL Stores	no default	required	<p>Determines whether you want to run Secure Socket Layer (SSL) with the demo SSL certificates or with your own custom keystore and truststore. Valid values are true or false.</p> <p>If Setup Server Custom SSL Stores is true, the following parameters must also be specified: Custom KeyStore Path, Custom KeyStore PassPhrase, Custom TrustStore Path, Custom TrustStore PassPhrase, and Private Key Alias.</p>
Start Managed Servers	true	optional	Specifies whether or not to start up the managed servers once they have been created. Valid values are true and false.

Additional Parameters Defined in this Step: Weblogic Managed Server Validate Parameters, continued

Parameter Name	Default Value	Required	Description
WLST Call Wrapper	no default	required	Command that will invoke the WebLogic Scripting Tool (WLST). For example:  <code>su &lt;user&gt; /opt/oracle/WebLogic/install/common/bin/wlst.sh</code>  The fully qualified path will vary depending on where you installed the product. The <user> must have appropriate permissions.
WebLogic User Id	no default	required	The WebLogic user that will be used to authenticate with the Administration Server.
WebLogic User Password	no default	required	The WebLogic password that will be used to authenticate with the Administration Server.

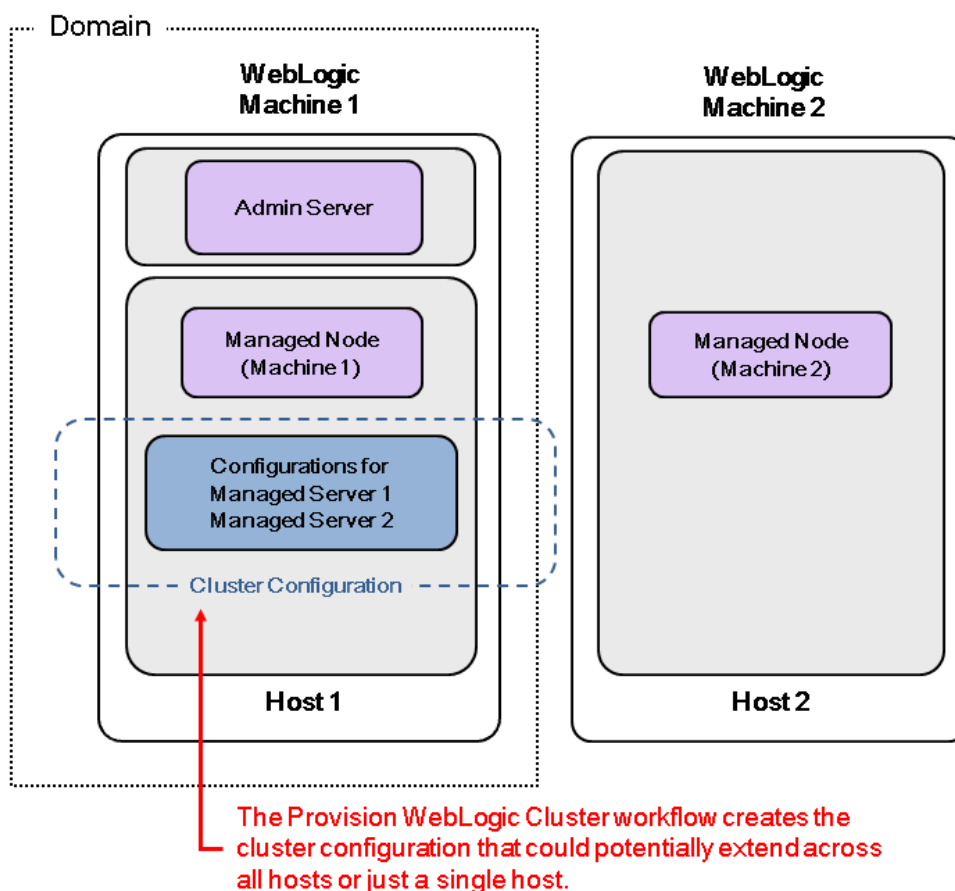
## Provision WebLogic Cluster

This workflow creates a WebLogic cluster configuration from an existing installation and domain of WebLogic and adds the existing Managed Servers to the cluster configuration.

This workflow is optional. Use it only if you want to organize your Managed Servers into a cluster. Clusters allow your WebLogic environment to be highly-available and load-balanced.

Your cluster can span the Managed Servers on a single machine (a vertical cluster) or across multiple machines (a horizontal cluster).

The following reference architecture diagram gives an example of what this workflow does:



Before you can run this workflow you need to have an operational WebLogic 11g or 12c environment.

For information about how this workflow can be used with other WebLogic provisioning workflows to create an operational WebLogic 11g or 12c environment, see [How to Use the Workflows Together](#) on page 19.

**Note:** If you do not plan to expand the domain, you should manually start the cluster after running this workflow.

You can specify input parameters to select either multicast or unicast cluster messaging mode for your cluster.

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

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

## Prerequisites for this Workflow

Be sure that the following prerequisites are satisfied before you run the [Provision WebLogic Cluster](#) workflow:

1. The latest HP DMA solution packs require the latest HP DMA platform. To use the latest solution packs, update the HP DMA platform. HP DMA 10.30 solution packs are supported on HP DMA 10.30 (and later).
2. You have installed the Application Server Provisioning Solution Pack.

For more information about prerequisites for WebLogic 11g and 12c, refer to the [WebLogic Product Documentation](#) on page 125.

## How this Workflow Works

The following information describes how the [Provision WebLogic Cluster](#) workflow works:

### Overview

The workflow does the following:

- Prepares to provision the WebLogic cluster by setting up the command to be used in subsequent steps and validating input parameters.
- Creates the cluster configuration using the WebLogic Scripting Tool (WLST): accesses the domain information, creates the cluster, sets the cluster messaging mode to either multicast or unicast, assigns the Managed Server (or servers) to the cluster, then updates the domain.
- Stops and restarts the WebLogic Administration Server.

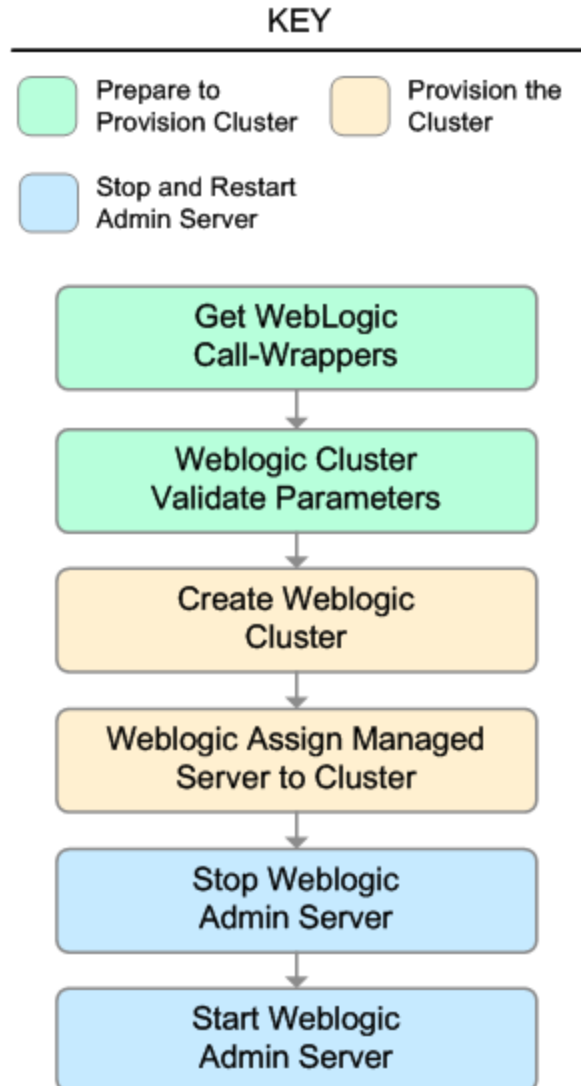
### Validation Checks Performed

Much of the validation centers on the input parameters:

- Checks that the BEA Home and WLS Install Home files exist.
- Verifies that Multicast Port is null or a valid integer.
- If either Multicast Address or Multicast Port are null then the cluster messaging mode will be set to unicast. Otherwise it will be set to multicast.

### Steps Executed

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



### Steps Used in Provision WebLogic Cluster

Workflow Step	Description
Get WebLogic Call-Wrappers	This step creates the commands that subsequent steps will use to execute scripts and WebLogic Scripting Tool (WLST) operations.
Weblogic Cluster Validate Parameters	This step prepares the parameters needed to create a cluster and add Managed Servers to the cluster on WebLogic.
Create Weblogic Cluster	This step creates a cluster from an existing domain and installation of WebLogic.
Weblogic Assign Managed Server to Cluster	This step adds Managed Servers to an existing cluster on WebLogic.
WebLogic Stop Admin Server	This step checks if the WebLogic Administration Server on a given machine or server is running. If it is running, the step stops it.
Start Weblogic Admin Server	This step starts the WebLogic Administration Server.

For parameter descriptions and defaults, see [Parameters for Provision WebLogic Cluster](#) on page 110.

## How to Run this Workflow

The following instructions show you how to customize and run the [Provision WebLogic Cluster](#) workflow in your environment.

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

The workflow provides default values for some parameters. These default values are usually sufficient for a "typical" installation. You can override the defaults by specifying parameter values in the deployment. You can also expose additional parameters in the workflow, if necessary, to accomplish more advanced scenarios. Any parameters not explicitly specified in the deployment will have the default values listed in [Parameters for Provision WebLogic Cluster](#) on page 110.

**Note:** Before following this procedure, review the [Prerequisites for this Workflow](#) on page 102, and ensure that all requirements are satisfied.

### To use the Provision WebLogic Cluster workflow:

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

#### Input Parameters for Get WebLogic Call-Wrappers

Parameter Name	Default Value	Required	Description
BEA Home	no default	required	Fully qualified path to the middleware home directory that contains the WebLogic installation. For example: <code>/opt/oracle/weblogic</code>
WLS Install Home	no default	required	Fully qualified path to the directory where WebLogic Server will be installed. For example: <code>/opt/oracle/weblogic/wlserver12.1</code>

#### Input Parameters for Weblogic Cluster Validate Parameters

Parameter Name	Default Value	Required	Description
Cluster Name	no default	required	The name of the new cluster. For example: <code>ClusterAppServer</code> .
Domain Path	no default	required	Fully qualified path where the domain and domain configuration will be created. For example: <code>/opt/weblogic/user_projects/domains</code>

#### Input Parameters for Weblogic Cluster Validate Parameters, continued

Parameter Name	Default Value	Required	Description
Managed Servers	no default	required	Comma-delimited list of the names of the Managed Server (or servers) that will be added to the new cluster. For example: AppServer1, AppServer2.
Multicast Address	no default	optional	The multicast address that will be used by cluster members to communicate with each other. Specify this ONLY if you intend to use multicast for cluster communication.
Multicast Port	no default	optional	The multicast port (between 1 and 65535) that will be used by cluster members to communicate with each other. Specify this ONLY if you intend to use multicast for cluster communication.

**Note:** See [Parameters for Provision WebLogic Cluster](#) on page 110 for detailed descriptions of all input parameters for this workflow, including default values.

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

**Note:** The target for this deployment should be set to the server where the WebLogic Administration Server is provisioned.

8. Save the deployment (click **Save** in the lower right corner).
9. Run the workflow using this deployment (see "Run Your Workflow" in *HP DMA Quick Start Tutorial* for instructions).

**Note:** If you do not plan to expand the domain, you should manually start the cluster after running this workflow.

#### To verify the results:

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

## Sample Scenario

This topic shows you typical parameter values for different use cases for the [Provision WebLogic Cluster](#) workflow.

### Scenario 1: To use multicast

If you intend to use multicast for cluster communication, set both Multicast Address and Multicast Port to appropriate values.

#### Input Parameters for Get WebLogic Call-Wrappers

Parameter Name	Example Value	Description
BEA Home	no default	Fully qualified path to the middleware home directory that contains the WebLogic installation. For example:  <code>/opt/oracle/weblogic</code>
WLS Install Home	no default	Fully qualified path to the directory where WebLogic Server will be installed. For example:  <code>/opt/oracle/weblogic/wlserver12.1</code>

#### Input Parameters for Weblogic Cluster Validate Parameters

Parameter Name	Example Value	Description
Cluster Name	see description	The name of the new cluster. For example: ClusterAppServer.
Domain Path	see description	Fully qualified path where the domain and domain configuration will be created. For example:  <code>/opt/weblogic/user_projects/domains</code>
Managed Servers	see description	Comma-delimited list of the names of the Managed Server (or servers) that will be added to the new cluster. For example: AppServer1, AppServer2.
Multicast Address	237.0.0.101	The multicast address that will be used by cluster members to communicate with each other. Specify this ONLY if you intend to use multicast for cluster communication.
Multicast Port	9200	The multicast port (between 1 and 65535) that will be used by cluster members to communicate with each other. Specify this ONLY if you intend to use multicast for cluster communication.

Be sure that the default values for all remaining input parameters are appropriate for your environment (see [Parameters for Provision WebLogic Cluster](#) on page 110).

### Scenario 2: To use unicast

If you intend to use unicast for cluster communication, do not set either Multicast Address or Multicast Port .

#### Input Parameters for Get WebLogic Call-Wrappers

Parameter Name	Example Value	Description
BEA Home	no default	Fully qualified path to the middleware home directory that contains the WebLogic installation. For example:  /opt/oracle/weblogic
WLS Install Home	no default	Fully qualified path to the directory where WebLogic Server will be installed. For example:  /opt/oracle/weblogic/wlserver12.1

#### Input Parameters for WebLogic Cluster Validate Parameters

Parameter Name	Example Value	Description
Cluster Name	see description	The name of the new cluster. For example: ClusterAppServer.
Domain Path	see description	Fully qualified path where the domain and domain configuration will be created. For example:  /opt/weblogic/user_projects/domains
Managed Servers	see description	Comma-delimited list of the names of the Managed Server (or servers) that will be added to the new cluster. For example: AppServer1, AppServer2.
Multicast Address		The multicast address that will be used by cluster members to communicate with each other. Specify this ONLY if you intend to use multicast for cluster communication.
Multicast Port		The multicast port (between 1 and 65535) that will be used by cluster members to communicate with each other. Specify this ONLY if you intend to use multicast for cluster communication.

Be sure that the default values for all remaining input parameters are appropriate for your environment (see [Parameters for Provision WebLogic Cluster](#) on the next page).

## Parameters for Provision WebLogic Cluster

The following tables describe the required and optional input parameters for this workflow. Some of these parameters may not be initially visible in a deployment (see [How to Expose Additional Workflow Parameters](#) on page 131). For some parameters, if you do not specify a value for a parameter, a default value is assigned.

Following are tables for each of the steps used by this workflow where parameters are defined:

### Parameters Defined in this Step: Get WebLogic Call-Wrappers

Parameter Name	Default Value	Required	Description
BEA Home	no default	required	Fully qualified path to the middleware home directory that contains the WebLogic installation. For example:  <code>/opt/oracle/weblogic</code>
WLS Install Home	no default	required	Fully qualified path to the directory where WebLogic Server will be installed. For example:  <code>/opt/oracle/weblogic/wlserver12.1</code>

### Additional Parameters Defined in this Step: Weblogic Cluster Validate Parameters

Parameter Name	Default Value	Required	Description
Call Wrapper	see description	optional	Command that will execute this step (or subsequent steps) as a specific user.  For UNIX targets, the default is: <code>/opt/hp/dma/client/jython.sh</code> running as root  For Windows targets, the default is: <code>jython</code> running as Administrator  <b>Caution:</b> This parameter is derived by the workflow. Under most circumstances, you should not change its mapping or its value.
Cluster Name	no default	required	The name of the new cluster. For example: <code>ClusterAppServer</code> .
Domain Path	no default	required	Fully qualified path where the domain and domain configuration will be created. For example:  <code>/opt/weblogic/user_projects/domains</code>
Managed Servers	no default	required	Comma-delimited list of the names of the Managed Server (or servers) that will be added to the new cluster. For example: <code>AppServer1, AppServer2</code> .

Additional Parameters Defined in this Step: Weblogic Cluster Validate Parameters, continued

Parameter Name	Default Value	Required	Description
Multicast Address	no default	optional	The multicast address that will be used by cluster members to communicate with each other. Specify this ONLY if you intend to use multicast for cluster communication.
Multicast Port	no default	optional	The multicast port (between 1 and 65535) that will be used by cluster members to communicate with each other. Specify this ONLY if you intend to use multicast for cluster communication.
WLST Call Wrapper	no default	required	<p>Command that will invoke the WebLogic Scripting Tool (WLST). For example:</p> <pre>su &lt;user&gt; /opt/oracle/WebLogic/install/ common/bin/wlst.sh</pre> <p>The fully qualified path will vary depending on where you installed the product. The &lt;user&gt; must have appropriate permissions.</p>

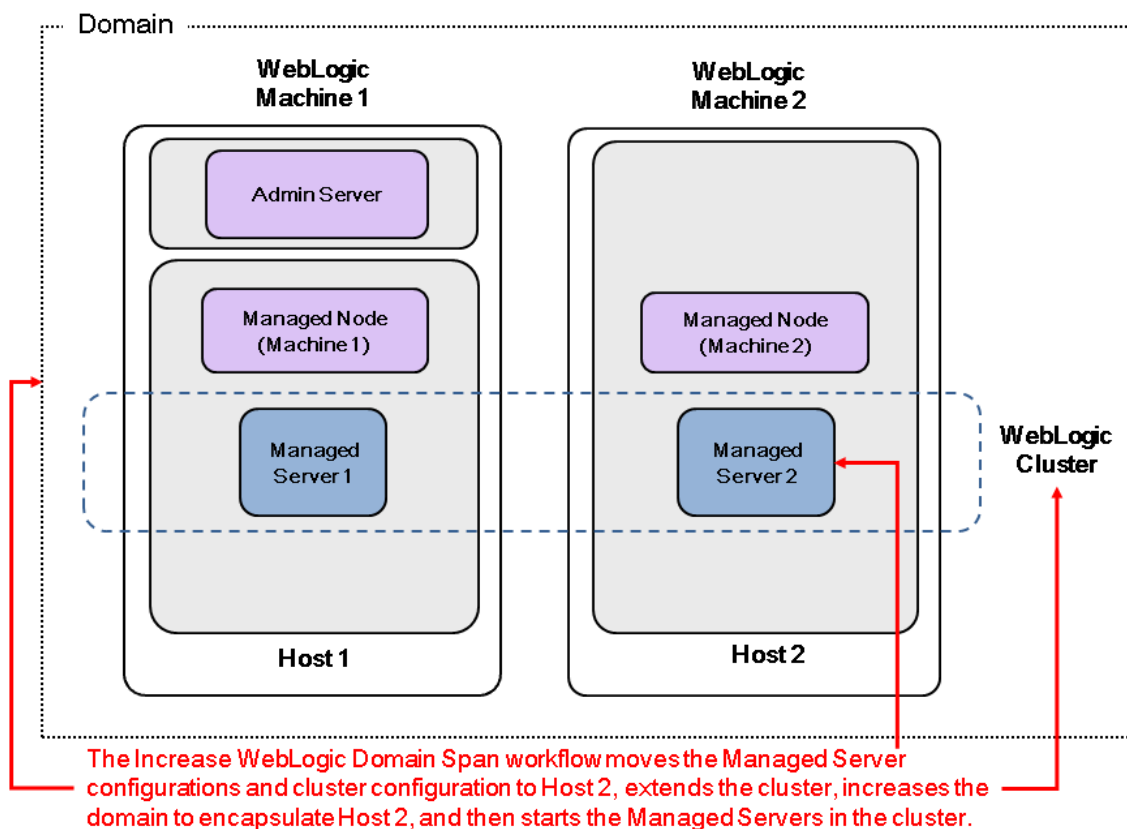
## Increase WebLogic Domain Span

This workflow increases the span of a WebLogic domain by adding other hosts to that domain. To accomplish this it moves the Managed Server configurations and cluster configuration to the other hosts, extends the cluster, starts the Managed Servers, and starts the cluster.

The basic process is to pack up the domain into a template file, send that file to the remote machines, and then unpack it into the correct locations.

This workflow is optional. Use it only if your domain spans more than one machine.

The following reference architecture diagram gives an example of what this workflow does:



Before you can run this workflow you need to have an operational WebLogic 11g or 12c with a horizontal cluster.

For information about how this workflow can be used with other WebLogic provisioning workflows to create an operational WebLogic 11g or 12c environment, see [How to Use the Workflows Together](#) on page 19.

**Note:** Before running this workflow set up the SSH keys between the original domain's machine and the target machine (or machines).

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

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

## Prerequisites for this Workflow

Be sure that the following prerequisites are satisfied before you run the [Increase WebLogic Domain Span](#) workflow:

1. The latest HP DMA solution packs require the latest HP DMA platform. To use the latest solution packs, update the HP DMA platform. HP DMA 10.30 solution packs are supported on HP DMA 10.30 (and later).
2. You have installed the Application Server Provisioning Solution Pack.
3. SSH keys are set up between the original domain's machine and the target machine (or machines). These shared keys set up Trust IDs to log in without a password.

For more information about prerequisites for WebLogic 11g and 12c, refer to the [WebLogic Product Documentation](#) on page 125.

## How this Workflow Works

The following information describes how the [Increase WebLogic Domain Span](#) workflow works:

### Overview

The workflow does the following:

- Sets up the command to be used to increase the WebLogic domain span.
- Uses the pack utility to pack up the domain into a template file, sends that file to the remote machine (or machines), then uses the unpack utility to unpack it into the correct location.

In more detail, this workflow uses the internal tool in WebLogic to jar up the configurations for the Managed Servers and the cluster configuration into an archive file. Then it pushes via Secure Copy (SCP) and moves the JAR file to the other machines. Finally, it uses the same utility to unjar the archive file onto the other machines.

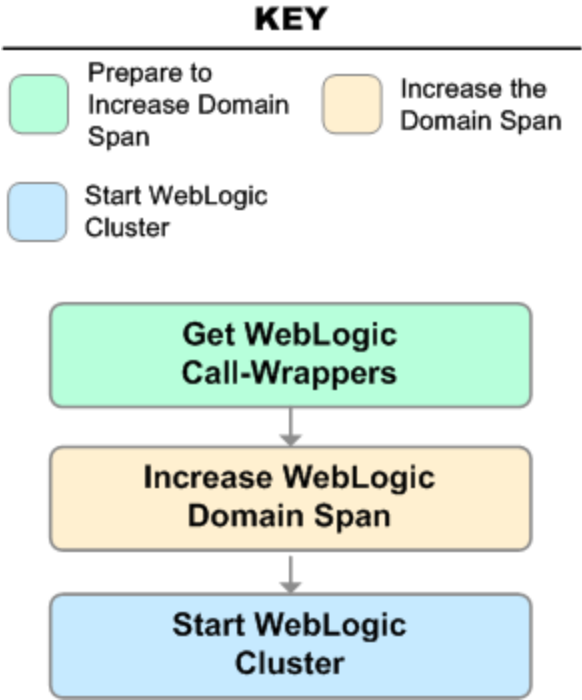
- Starts up the cluster in the WebLogic domain.

### Validation Checks Performed

This workflow checks that the BEA Home and WLS Install Home files exist.

Steps Executed

The Increase WebLogic Domain Span workflow includes the following steps. Each step must complete successfully before the next step can start. If a step fails, the workflow reports a failure and all subsequent steps are skipped.



Steps Used in Increase WebLogic Domain Span

Workflow Step	Description
Get WebLogic Call-Wrappers	This step creates the commands that subsequent steps will use to execute scripts and WebLogic Scripting Tool (WLST) operations.
Increase WebLogic Domain Span	This step uses the pack and unpack utilities within the WebLogic product to pack up the domain configuration and unpack it on a remote target machine (or machines).
Start WebLogic Cluster	This step starts up the cluster in the WebLogic domain.

For parameter descriptions and defaults, see [Parameters for Increase WebLogic Domain Span](#) on page 122.

## How to Run this Workflow

The following instructions show you how to customize and run the [Increase WebLogic Domain Span](#) workflow in your environment.

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

The workflow provides default values for some parameters. These default values are usually sufficient for a "typical" installation. You can override the defaults by specifying parameter values in the deployment. You can also expose additional parameters in the workflow, if necessary, to accomplish more advanced scenarios. Any parameters not explicitly specified in the deployment will have the default values listed in [Parameters for Increase WebLogic Domain Span](#) on page 122.

**Note:** Before following this procedure, review the [Prerequisites for this Workflow](#) on page 114, and ensure that all requirements are satisfied.

### To use the Increase WebLogic Domain Span workflow:

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

#### Input Parameters for Get WebLogic Call-Wrappers

Parameter Name	Default Value	Required	Description
BEA Home	no default	required	Fully qualified path to the middleware home directory that contains the WebLogic installation. For example: <code>/opt/oracle/weblogic</code>
WLS Install Home	no default	required	Fully qualified path to the directory where WebLogic Server will be installed. For example: <code>/opt/oracle/weblogic/wlserver12.1</code>

#### Input Parameters for Increase WebLogic Domain Span

Parameter Name	Default Value	Required	Description
Local Domain Path	no default	required	Path to the local domain. If the specified path is a relative path, it is assumed to be relative to BEA Home. For example: <code>/opt/oracle/weblogic/user_projects/domains/base_domain</code> where <code>/opt/oracle/weblogic</code> is the BEA Home.

#### Input Parameters for Increase WebLogic Domain Span, continued

Parameter Name	Default Value	Required	Description
Local Template Path	no default	required	Path to the local template directory or the path to a template file. If the specified path is a relative path, it is assumed to be relative to BEA Home. For example:  /opt/oracle/weblogic/user_projects/domains/base_domain.jar  where /opt/oracle/weblogic is the BEA Home.
Remote Addresses	no default	required	Comma-delimited list of hosts (DNS addresses or IP addresses) that the domain will span.

#### Input Parameters for Start WebLogic Cluster

Parameter Name	Default Value	Required	Description
Admin Server Port	no default	optional	The non-SSL port on which the WebLogic Administration Server will run.
Cluster Name	no default	required	The name of the new cluster. For example: ClusterAppServer.
Weblogic Admin Password	no default	required	The password that will be used to authenticate with the WebLogic Administration Server.
WebLogic Admin User	weblogic	required	The WebLogic administrator account that will be used to authenticate with the Administration Server.

**Tip:** To avoid having to re-enter passwords whenever they change, you can create a policy to provide them to the workflow (see [How to Use a Policy to Specify Parameter Values](#) on page 132).

**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 [How to Expose Additional Workflow Parameters](#) on page 131

See [Parameters for Increase WebLogic Domain Span](#) on page 122 for detailed descriptions of all input parameters for this workflow, including default values.

3. In the workflow editor, expose any additional parameters that you need. You will specify values for those parameters when you create the deployment.
4. Save the changes to the workflow (click **Save** in the lower right corner).
5. Create a new deployment (see "Create a Deployment" in *HP DMA Quick Start Tutorial* for instructions).
6. On the Parameters tab, specify values for the required parameters listed in step 2 and any

additional parameters that you have exposed. You do not need to specify values for those parameters whose default values are appropriate for your environment.

7. On the Targets tab, specify one or more targets for this deployment.

**Note:** The target for this deployment should be set to the server where the WebLogic Administration Server is provisioned.

The workflow pushes the configuration over to other hosts based on your input parameters.

8. Save the deployment (click **Save** in the lower right corner).
9. Run the workflow using this deployment (see "Run Your Workflow" in *HP DMA Quick Start Tutorial* for instructions).

**To verify the results:**

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

*Optional:* If you want to further verify the results:

1. View the `{BEAHOME}/logs/log.txt` file.  
This file is created after the installation is complete.
2. Look for specific information about what was installed.

## Sample Scenario

It is very straightforward to run the [Increase WebLogic Domain Span](#) workflow. This topic shows you typical parameter values to use.

### Typical parameters:

#### Input Parameters for Get WebLogic Call-Wrappers

Parameter Name	Example Value	Description
BEA Home	see description	Fully qualified path to the middleware home directory that contains the WebLogic installation. For example:  <code>/opt/oracle/weblogic</code>
WLS Install Home	see description	Fully qualified path to the directory where WebLogic Server will be installed. For example:  <code>/opt/oracle/weblogic/wlserver12.1</code>

#### Input Parameters for Increase WebLogic Domain Span

Parameter Name	Example Value	Description
Local Domain Path	see description	Path to the local domain. If the specified path is a relative path, it is assumed to be relative to BEA Home. For example:  <code>/opt/oracle/weblogic/user_projects/domains/base_domain</code> where <code>/opt/oracle/weblogic</code> is the BEA Home.
Local Template Path	see description	Path to the local template directory or the path to a template file. If the specified path is a relative path, it is assumed to be relative to BEA Home. For example:  <code>/opt/oracle/weblogic/user_projects/domains/base_domain.jar</code> where <code>/opt/oracle/weblogic</code> is the BEA Home.
Remote Addresses	server. company.com	Comma-delimited list of hosts (DNS addresses or IP addresses) that the domain will span.

#### Input Parameters for Start WebLogic Cluster

Parameter Name	Example Value	Description
Admin Server Port	8001	The non-SSL port on which the WebLogic Administration Server will run.
Cluster Name	see description	The name of the new cluster. For example: ClusterAppServer.

Be sure that the default values for all remaining input parameters are appropriate for your environment (see [Parameters for Increase WebLogic Domain Span](#) on the next page).

## Parameters for Increase WebLogic Domain Span

The following tables describe the required and optional input parameters for this workflow. Some of these parameters may not be initially visible in a deployment (see [How to Expose Additional Workflow Parameters](#) on page 131). For some parameters, if you do not specify a value for a parameter, a default value is assigned.

Following are tables for each of the steps used by this workflow where parameters are defined:

### Parameters Defined in this Step: Get WebLogic Call-Wrappers

Parameter Name	Default Value	Required	Description
BEA Home	no default	required	Fully qualified path to the middleware home directory that contains the WebLogic installation. For example:  <code>/opt/oracle/weblogic</code>
WLS Install Home	no default	required	Fully qualified path to the directory where WebLogic Server will be installed. For example:  <code>/opt/oracle/weblogic/wlserver12.1</code>

### Additional Parameters Defined in this Step: Increase WebLogic Domain Span

Parameter Name	Default Value	Required	Description
Call Wrapper	see description	optional	Command that will execute this step (or subsequent steps) as a specific user.  For UNIX targets, the default is: <code>/opt/hp/dma/client/jython.sh</code> running as root  For Windows targets, the default is: <code>jython</code> running as Administrator  <b>Caution:</b> This parameter is derived by the workflow. Under most circumstances, you should not change its mapping or its value.
Local Domain Path	no default	required	Path to the local domain. If the specified path is a relative path, it is assumed to be relative to BEA Home. For example:  <code>/opt/oracle/weblogic/user_projects/domains/base_domain</code>  where <code>/opt/oracle/weblogic</code> is the BEA Home.

#### Additional Parameters Defined in this Step: Increase WebLogic Domain Span, continued

Parameter Name	Default Value	Required	Description
Local Template Path	no default	required	Path to the local template directory or the path to a template file. If the specified path is a relative path, it is assumed to be relative to BEA Home. For example:  <code>/opt/oracle/weblogic/user_projects/domains/base_domain.jar</code>  where <code>/opt/oracle/weblogic</code> is the BEA Home.
Remote Addresses	no default	required	Comma-delimited list of hosts (DNS addresses or IP addresses) that the domain will span.
Remote Domain Path	no default	optional	Path where the domain will be placed on the remote machine. If the specified path is a relative path, it is assumed to be relative to BEA Home.
Remote Template Path	no default	optional	Path to the remote template directory or the path to a template file. If the specified path is a relative path, it is assumed to be relative to BEA Home. This parameter defaults to Local Template Path.

#### Additional Parameters Defined in this Step: Start WebLogic Cluster

Parameter Name	Default Value	Required	Description
Admin Server Port	no default	optional	The non-SSL port on which the WebLogic Administration Server will run.
Cluster Name	no default	required	The name of the new cluster. For example: <code>ClusterAppServer</code> .
WLST Call Wrapper	no default	required	Command that will invoke the WebLogic Scripting Tool (WLST). For example:  <code>su &lt;user&gt; /opt/oracle/WebLogic/install/common/bin/wlst.sh</code>  The fully qualified path will vary depending on where you installed the product. The <code>&lt;user&gt;</code> must have appropriate permissions.  <b>Caution:</b> This parameter is derived by the workflow. Under most circumstances, you should not change its mapping or its value.
Weblogic Admin Password	no default	required	The password that will be used to authenticate with the WebLogic Administration Server.

Additional Parameters Defined in this Step: Start WebLogic Cluster, continued

Parameter Name	Default Value	Required	Description
WebLogic Admin User	weblogic	required	The WebLogic administrator account that will be used to authenticate with the Administration Server.

## Chapter 3: Reference Information

This chapter contains the following information:

Topic	Description
<a href="#">WebLogic Product Documentation</a>	Links to current product documentation for WebLogic 11g and 12c
<a href="#">HP DMA Documentation</a>	Links to additional HP DMA documentation

### WebLogic Product Documentation

For product documentation for WebLogic 11g and 12c, see:

<http://www.oracle.com/technetwork/middleware/weblogic/documentation/index.html>

For the current list of hardware and software requirements, as well as supported platforms for WebLogic 11g and 12c, see:

<http://www.oracle.com/technetwork/middleware/weblogic/documentation/index.html>

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

### HP DMA Documentation

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

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

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

# Chapter 4: Tips and Best Practices

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

- [How a Solution Pack is Organized](#) on the next page
- [How to Expose Additional Workflow Parameters](#) on page 131
- [How to Use a Policy to Specify Parameter Values](#) on page 132
- [How to Import a File into the Software Repository](#) on page 135

# How a Solution Pack is Organized

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

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

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

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

The screenshot displays the HP Database & Middleware Automation console. The top navigation bar includes links for Home, Automation, Reports, Environment, Solutions, and Setup. Below this, a secondary bar shows Workflows, Steps, Functions, Policies, Deployments, Run, Console, and History. The main content area is titled 'My Copy of Run Oracle Compliance Audit' and features several tabs: Documentation (selected), Workflow, History, Deployments, and Roles. Under the Documentation tab, there are input fields for Name (pre-filled with 'My Copy of Run Oracle Compliance Audit'), Tags, Type (set to 'Oracle'), and Target level (set to 'Instance'). Below these fields is a 'Documentation:' section containing three expandable panels: 'Purpose', 'Description', and 'Parameters'. The 'Purpose' panel describes auditing an Oracle Database instance against CIS benchmarks and PCI/SOX requirements. The 'Description' panel details the workflow's process, including CIS Level 1 and 2 auditing and report generation. The 'Parameters' panel is currently collapsed. At the bottom of the console, there is a toolbar with icons for DELETE, EXPORT, EXTRACT POLICY, and DEPLOY, along with buttons for Copy, Save, and CANCEL.

HP Database & Middleware Automation

Home Automation Reports Environment Solutions Setup

Workflows Steps Functions Policies Deployments Run Console History

### My Copy of Run Oracle Compliance Audit

Documentation Workflow History Deployments Roles

Name: My Copy of Run Oracle Compliance Audit

Tags:

Type: Oracle

Target level: Instance

Documentation:

**Purpose**

Audit an Oracle Database instance for compliance with the following Center for Internet Security (CIS) benchmarks and, optionally, compare the audit results to the related PCI and SOX requirements:

- CIS Security Configuration Benchmark for Oracle Database Server 11g, version 1.1.0, December 2011
- CIS Security Benchmark for Oracle 9i/10g, version 2.01, April 2005
- Payment Card Industry (PCI) Data Security Standard Version 2.0, October 2010
- Sarbanes-Oxley (SOX) Sarbanes-Oxley Act of 2002 Section 302

**Description**

This workflow will audit an Oracle Database instance using CIS Level 1 and Level 2 auditing. It will then compare the results to the pertinent PCI and SOX requirements, where applicable. This audit, which runs in conjunction with the HP DMA reporting tool, can identify more than 175 compliance related problems with an Oracle database. You can view information about the audit on the Console while the audit is running. After the audit has finished, the workflow sends a summary report to each specified email address. You can also view a compliance report on the Reports page.

**Parameters**

HELP PDF EDIT

DELETE EXPORT EXTRACT POLICY DEPLOY Copy Save or CANCEL

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

hp Database & Middleware Automation

Home

Automation

Reports

Environment

Solutions

Setup

Workflows

Steps

Functions

Policies

Deployments

Run

Console

History

Get Oracle Home

General

Action

Parameters

History

Workflows

Solutions

Roles

Properties

Name: Get Oracle Home

Tags:

Type: Oracle

Category: Script

Targetable:☐

Documentation

Description:

Get the value of ORACLE\_HOME from the appropriate source:

- The /etc/oratab or /var/opt/oracle/oratab file on UNIX

- The registry on Windows

Dependencies: None

Input Parameters: None

Output Parameters:

- Oracle Home = The fully qualified name of the ORACLE\_HOME

- Oracle SID = The Oracle server (instance) ID

Return Code:

0 = Step was successful

Copy

THIS STEP IS READ ONLY

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

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

hp Database & Middleware Automation

Home

Automation

Reports

Environment

Solutions

Setup

Workflows

Steps

Functions

Policies

Deployments

Run

Console

History

Parse Oracle Inventory

General

Action

Parameters

History

Workflows

Solutions

Roles

Parameters

INPUT PARAMETERS

ADD

Inventory Files

×

Oracle Account

×

Oracle Home

×

Server Wrapper

×

OUTPUT PARAMETERS

ADD

CRS Account

×

CRS Active Version

×

CRS Group

×

CRS Home

×

CRS Home Name

×

CRS Nodes

×

Cluster Nodes

×

Inventory Groups

×

Inventory Locations

×

✕ Parameter is in use and cannot be removed.

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

Get Listener Names / Oracle SIDs

Optional: Comma delimited list of ORACLE\_SIDs, at least one of which a resulting listener must service. If blank, listeners are not limited to those servicing any specific ORACLE\_SID.

7

Prepare Oracle Instance

0

3, 8

8

Get Listener Names

0

3, 9

Listener Homes: Prepare Oracle Instance.Oracle Home

Oracle SIDs: Get Oracle Home.Oracle SID

9

Audit Unix or Linux OS Specific Settings

0

3, 10

10

Audit Installation and Patch

0

11, 12

Click here

To see the parameter description here

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

HP Database & Middleware Automation

Home

Automation

Reports

Environment

Solutions

Setup

Workflows

Steps

Functions

Policies

Deployments

Run

Console

History

Run Oracle Compliance CIS

Targets

Parameters

Roles

Gather Parameters for Oracle Compliance

Compliance Type: CIS

Fixed Value

Compliance type that will be audited by the workflow. Compliance types supported: CIS, PCI, SOX. Will be defaulted to CIS.

Excluded Compliance Checks:

Fixed Value

Optional: Checks to exclude from of Compliance Checks

Inventory Files: /etc/orainst.loc

Fixed Value

Optional: Comma separated list of fully qualified Oracle inventory files. If not specified, default to /etc/orainst.loc, /var/opt/oracle/orainst.loc, or %ProgramFiles%\OracleInventory.

Gather Advanced Parameters for Oracle Compliance

Email Addresses to Receive Report: CISComplianceAuditor@mycompany.com

Fixed Value

\*Optional. Provided an email address or multiple email addresses separated by commas without spaces that you would like to receive an email of the results of the compliance tests run against the target specified.

DELETE

RUN

Restore defaults

Copy

Save

CANCEL


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




## How to Expose Additional Workflow Parameters

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

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

### To expose a hidden workflow parameter:

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

Step	Name	Required Result	Next
▼ 1	<a href="#">Gather Parameters for Oracle Compliance</a>		2
	Compliance Type: - User selected -		
	Excluded Compliance Checks: - User selected -		
	Inventory Files: - User selected -		

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

# How to Use a Policy to Specify Parameter Values

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

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

To establish a policy, you can either [Create a Policy](#) or [Extract a Policy](#) from a workflow.

After you establish the policy, you must [Reference the Policy in the Deployment](#).

For more information, see the *HP DMA User Guide*. This document is available on the HP Software Support web site: <https://softwaresupport.hp.com/>

## Create a Policy

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

### To create a policy that provides parameter values:

1. In the HP DMA web UI, go to Automation > Policies.
2. Click **New Policy**.
3. In the **Name** box, specify the name of the policy
4. For each parameter value that you want to provide using this policy, perform the following actions on the Attributes tab:
  - a. From the drop-down list, select the type of attribute:
    - A Text attribute contains simple text that users can view while deploying and running workflows.
    - A List attribute contains a comma-separated list of values (or a large amount of text not suitable for a Text attribute).
    - A Password attribute contains simple text, but the characters are masked so that users cannot see the text.
  - b. In the text box to the left of the Add button, specify the name of the attribute.  
For your convenience, this name should be similar to the parameter name used in the pertinent workflow (or workflows).
  - c. Click **Add**.
  - d. In the new text box to the right of the attribute's name, enter a value for this attribute.  
To remove an attribute, click the **Remove** button.
5. On the Roles tab, grant Read and Write permission to any additional users and groups who will be

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

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

## Extract a Policy

An alternative to creating your own policy one attribute at a time is to extract the policy. This automatically creates a reusable policy that provides values for all input parameters associated with a workflow. This is a convenient way to create a policy.

### To extract a policy:

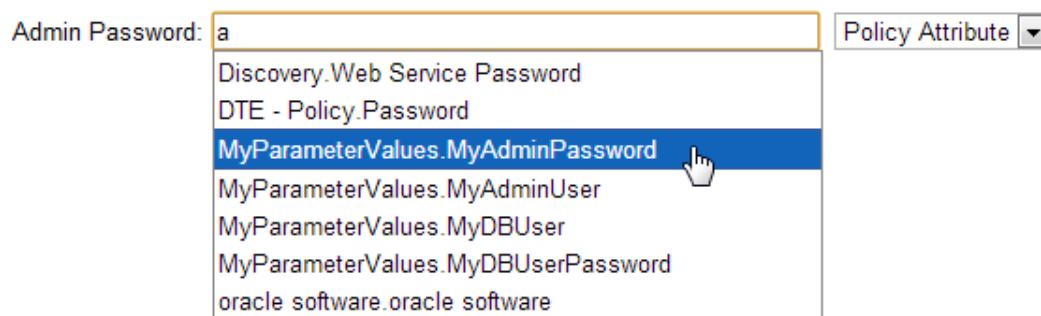
1. Go to Automation > Workflows.
2. Select the Workflow that you want to work with.
3. Click the Extract Policy link at the bottom of the screen.
4. Specify values for each attribute listed.
5. *Optional:* Remove any attributes that you do not want to use.
6. *Optional:* Add any new attributes that you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

## Reference the Policy in the Deployment

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

### To reference policy attributes in a deployment:

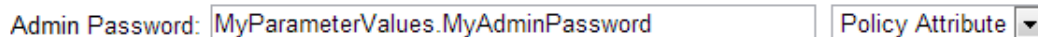
1. Create or access the deployment.  
See “Deployments” in the *HP DMA User Guide* for details.
2. On the Parameters tab, perform the following steps for each parameter whose value you want to provide by referencing a policy attribute:
  - a. In the drop-down menu for that parameter, select **Policy Attribute**.
  - b. In the text box for that parameter, type any character. A drop-down list of policy attributes appears. For example:



The screenshot shows a form with a label "Admin Password:" followed by a text input field containing the letter "a". To the right of the input field is a dropdown menu currently set to "Policy Attribute". Below the input field, a list of policy attributes is displayed. A mouse cursor is pointing at the attribute "MyParameterValues.MyAdminPassword".

Policy Attribute
Discovery.Web Service Password
DTE - Policy.Password
<b>MyParameterValues.MyAdminPassword</b>
MyParameterValues.MyAdminUser
MyParameterValues.MyDBUser
MyParameterValues.MyDBUserPassword
oracle software.oracle software

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



The screenshot shows the same form as before, but now the text input field for "Admin Password:" contains the value "MyParameterValues.MyAdminPassword". The dropdown menu remains set to "Policy Attribute".

Policy Attribute
MyParameterValues.MyAdminPassword

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

# How to Import a File into the Software Repository

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

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

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

## To import a file into the HP SA Software Library:

1. Launch the HP SA Client from the Windows Start Menu.  
By default, the HP SA Client is located in Start → All Programs → HP Business Service Automation → HP Server Automation Client  
If the HP SA Client is not installed locally, follow the instructions under “Installing the SA Client Launcher” in the *User Guide: Server Automation*, available on the HP Software Support web site: <https://softwaresupport.hp.com/>
2. In the navigation pane in the HP SA Client, select Library → By Folder.
3. Select (or create) the folder where you want to store the file.
4. From the Actions menu, select **Import Software**.
5. In the Import Software dialog, click the **Browse** button to the right of the File(s) box.
6. In the Open dialog:
  - a. Select the file (or files) to import.
  - b. Specify the character encoding to be used from the Encoding drop-down list. The default encoding is English ASCII.
  - c. Click **Open**. The Import Software dialog reappears.
7. From the Type drop-down list, select **Unknown**.
8. If the folder where you want to store the files does not appear in the Folder box, follow these steps:
  - a. Click the **Browse** button to the right of the Folder box.
  - b. In the Select Folder window, select the import destination location, and click **Select**. The Import Software dialog reappears.
9. From the Platform drop-down list, select all the operating systems listed.
10. Click **Import**.  
If one of the files that you are importing already exists in the folder that you specified, you will be prompted regarding how to handle the duplicate file. Press F1 to view online help that explains the options.
11. Click **Close** after the import is completed.

# Chapter 5: Troubleshooting

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

- [Target Type](#) below
- [User Permissions and Related Requirements](#) below
- [Discovery in HP DMA](#) on the next page

## Target Type

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

## User Permissions and Related Requirements

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

Roles are assigned by the HP Server Automation administrator. They are then registered in HP DMA by your HP DMA administrator.

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

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

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

For more information, see the *HP DMA Administrator Guide*. This document is available on the HP Software Support web site: <https://softwaresupport.hp.com/>

## Discovery in HP DMA

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

You must explicitly initiate the process of discovery—it is not automatic. See the *HP DMA User Guide* for instructions. This document is available on the HP Software Support web site:

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

# Glossary

## A

---

### **automation items**

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

## B

---

### **bridged execution**

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

## C

---

### **capability**

Capabilities are collections of related privileges. There are three capabilities defined in HP DMA. Login Access capability enables a user to log in to the web interface. This capability does not guarantee that this user can view any organizations or automation items—permissions are required to access those items. Workflow Creator

capability enables a user to create new workflows and make copies of other workflows. Administrator capability enables a user to perform any action and view all organizations. If you have Administrator capability, you do not need Workflow Creator capability. The Administrator can assign any of these capabilities to one or more roles registered roles.

### **connector**

HP DMA includes a Connector component that enables it to communicate with HP Server Automation. You must configure the Connector before you can run a workflow against a target.

### **cross-platform**

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

### **custom field**

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

## D

---

### **deployment**

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

## F

---

### **function**

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

## I

---

### **input parameters**

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

## M

---

### **mapping**

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

## O

---

### **organization**

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

## P

---

### **parameters**

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

### **policy**

Policies are reusable sets of attributes that can be used as parameter values in deployments. Deployments can reference policy attributes to change the automation behavior. Policies provide values for input parameters. They can contain fixed values or reference Custom Fields. Policies enable HP DMA to manage groups of hundreds or thousands of servers at a time without the need to configure each individual server.

## R

---

### **raw devices**

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

address space to the operating system kernel buffers.

### **role**

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

## **S**

---

### **smart group**

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

### **software repository**

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

### **solution pack**

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

### **steps**

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

## **T**

---

### **target instance**

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

## **W**

---

### **workflow**

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

### **workflow editor**

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

### **workflow templates**

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