Lifecycle Manager Installation and Configuration Guide

vCenter Lifecycle Manager 1.2

This document supports the version of each product listed and supports all subsequent versions until the document is replaced by a new edition. To check for more recent editions of this document, see http://www.vmware.com/support/pubs.

vmware®

You can find the most up-to-date technical documentation on the VMware Web site at:

http://www.vmware.com/support/

The VMware Web site also provides the latest product updates.

If you have comments about this documentation, submit your feedback to:

docfeedback@vmware.com

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

Contents

Installing and Configuring LCM

Upgrading Orchestrator and LCM

About This Book

The *Lifecycle Manager Installation and Configuration Guide* provides information about installing and configuring VMware® vCenter Lifecycle Manager (LCM).

Intended Audience

This book is intended for administrators who are installing and configuring LCM. The information in this guide is written for experienced system administrators who are familiar with virtual machine technology.

VMware Technical Publications Glossary

VMware Technical Publications provides a glossary of terms that might be unfamiliar to you. For definitions of terms as they are used in VMware technical documentation, go to http://www.vmware.com/support/pubs.

Document Feedback

VMware welcomes your suggestions for improving our documentation. If you have comments, send your feedback to docfeedback@vmware.com.

Technical Support and Education Resources

The following technical support resources are available to you. To access the current version of this book and other books, go to http://www.vmware.com/support/pubs.

Online and Telephone Support	To use online support to submit technical support requests, view your product and contract information, and register your products, go to http://www.vmware.com/support.
	Customers with appropriate support contracts should use telephone support for the fastest response on priority 1 issues. Go to http://www.vmware.com/support/phone_support.html.
Support Offerings	To find out how VMware support offerings can help meet your business needs, go to http://www.vmware.com/support/services.
VMware Professional Services	VMware Education Services courses offer extensive hands-on labs, case study examples, and course materials designed to be used as on-the-job reference tools. Courses are available onsite, in the classroom, and live online. For onsite pilot programs and implementation best practices, VMware Consulting

Services provides offerings to help you assess, plan, build, and manage your virtual environment. To access information about education classes, certification programs, and consulting services, go to http://www.vmware.com/services.

Introducing LCM

Understanding LCM

<div style="text-align: right;">**1**</div>

VMware vCenter Lifecycle Manager (LCM) automates the process of creating virtual machines and removing them from service at the appropriate time.

Using LCM, you can perform the following tasks:

- Handle and process virtual machine requests in a Web user interface.

- Automatically place servers based on their location, organization, environment, service level, or performance levels. When a solution is found for a set of criteria, the machine is automatically deployed.

- Enforce automatic deployment and configuration to reduce errors and speed up provisioning processes.

- Track lifecycle information for requested machines. Tracking helps maintain on-time archiving and deletion of end-of-life servers and avoids server sprawl.

This chapter includes the following topics:

- "Lifecycle Manager Process," on page 11

- "Lifecycle Manager Terminology," on page 13

- "Role-Based User Interface," on page 13

- "User Roles and Permitted Tasks," on page 14

- "LCM Administrator," on page 14

- "Lifecycle Manager Architecture," on page 15

Lifecycle Manager Process

LCM automates the process of creating virtual machines and removing them from service at the appropriate time.

Figure 1-1 provides an overview of the process and the tasks completed by each role.

Figure 1-1. Stages in the Lifecycle of a Virtual Machine under LCM
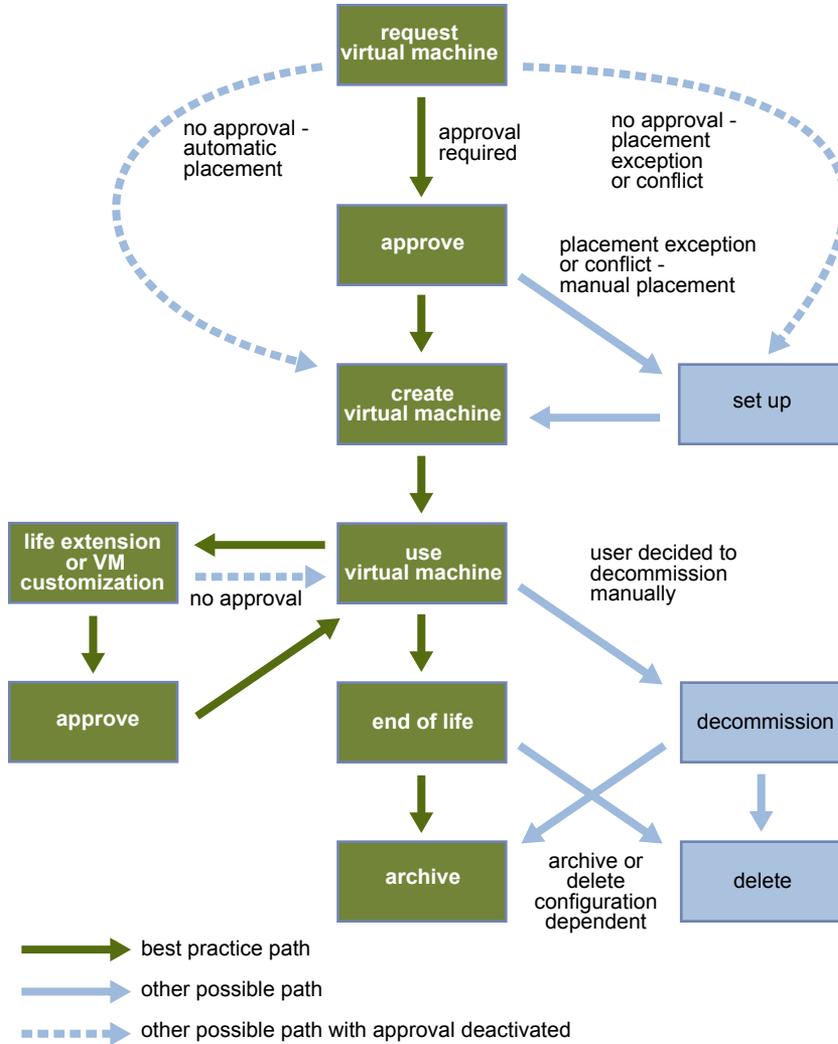
The way that LCM handles requests to create virtual machines depends on how the LCM Administrator has configured the approval process. If approval is required, an email notification is sent to the LCM Approver. If approval is not required, and there is no conflict with the request, the virtual machine is created. If there is a conflict, an LCM IT Staff user receives an email notification that a virtual machine is waiting to be created.

After a virtual machine is created, it can be used until the decommissioning date. Five days before the decommissioning date, an email notice is sent to the user who requested the virtual machine if email notifications are enabled. The requester can do one of the following:

■   Request to extend the life of the machine.

     If the extension is not approved, the virtual machine is decommissioned and is archived or deleted. The LCM Administrator determines whether decommissioned virtual machines are archived.

■   Manually decommission the virtual machine.

The LCM Administrator can choose to delete the virtual machine request. The LCM Administrator is the only role that can remove information about a virtual machine. When a request is deleted, no information about the virtual machine appears in reports, but the virtual machine is not deleted. If a virtual machine request is accidentally deleted, the LCM Administrator can recover the associated virtual machine.

Lifecycle Manager Terminology

LCM uses specific terminology to describe lifecycle events and attributes.

Commission	The creation of a requested virtual machine. The commission time is submitted during the request process.
Decommission	The requested machine reaches the end of its life. A decommission date is submitted during the request process. The decommissioned machine can be archived or deleted.
Extension	Extending the life of a virtual machine that is to be decommissioned. If approval is required, the request for extension must be approved before the owner of the virtual machine can continue to use it.
Infrastructure	Attributes such as the network, domain, and datastore affect where the requested virtual machine is placed in VMware Infrastructure.
Criteria	Attributes attached to a requested virtual machine that are selected during the request process, such as location, organization, server environment, service level, and performance. The LCM Administrator maps this information to the infrastructure.
Template Profile	The profile that is used when a requested virtual machine is cloned.
Customization Template	The template that determines the resources that the requested virtual machine uses, such as memory reservation, memory limit, CPU shares, and disk shares. Only the LCM IT Staff, LCM Tech Requester, and LCM Administrator can modify the customization template.
Placing	The requested virtual machine is created or moved into the infrastructure, based on the selected criteria and infrastructure.

Role-Based User Interface

LCM has a role-based interface. Users are presented only the options that are relevant to their specific role. All roles can request a virtual machine.

LCM users can be assigned the following roles:

LCM Administrator	Establishes the criteria used for machine placement and determines how the criteria convert to sizing or placement values. The LCM Administrator configures LCM and establishes the placement of virtual machines.
LCM Requester	Can request to extend the life of a created virtual machine. Requesters can power virtual machines on and off, as well as delegate this control to other users.
LCM Tech Requester	In addition to doing everything that the requester role can do, the LCM Tech Requester can customize the settings for the CPU, memory, and shares of the virtual machine.
LCM Approver	Approves virtual machine deployment and extension requests.
LCM IT Staff	Completes manual placement of approved virtual machines. If a machine cannot be placed based on the provided criteria, a user with the LCM IT Staff role must manually choose the sizing and placement of the new machine.

For more information on the tasks that users can perform, see the *Lifecycle Manager User's Guide*.

User Roles and Permitted Tasks

Every LCM user role can perform a certain set of tasks. The LCM Administrator can perform all tasks.

Table 1-1 describes how roles are mapped to tasks. Tasks marked with an O can be performed only by the owner of the request.

Table 1-1. Roles and Permitted Tasks

	LCM Admin	LCM IT Staff	LCM Approver	LCM Tech Requester	LCM Requester
Create infrastructure elements	X				
Map infrastructure elements with criteria	X				
Configure email notifications	X				
Generate reports	X	X	X		
Request virtual machines	X	X	X	X	X
Cancel virtual machine requests	O	O	O	O	O
Change state of virtual machine requests	X				
Change rights for virtual machine requests	X				
Approve virtual machine requests	X		X		
Set up virtual machines	X	X			
Retry placing failed virtual machine requests	X	X			
Validate virtual machine requests manually	X	X			
Check infrastructure for virtual machine requests	X	X			
Request extensions	X	O	O	O	O
Approve extensions	X		X		
Choose customization templates	X	O		O	
Approve customization templates	X	X			
Approve customization change requests	X	X	X		
Decommission virtual machines	X	O	O	O	O
Delete a request or a token	X				

LCM Administrator

The LCM Administrator sets up the LCM environment, and can perform all tasks that other user roles can perform.

The LCM Administrator is responsible for the following tasks.

- Configuring LCM
- Determining the infrastructure, such as the server environment
- Setting up email notifications, the look and feel of the user interface, and style sheets
- Specifying who can access elements such as resource pools or datastores

Lifecycle Manager Architecture

LCM is powered by VMware vCenter Orchestrator 4.1. Orchestrator is a development and process-automation platform that provides a library of extensible workflows for creating and running automated, configurable processes to manage the VMware vCenter infrastructure. You can use Orchestrator to create custom workflows that you can run from LCM.

Orchestrator exposes every operation in the vCenter Server API, allowing users to integrate all these operations into their automated processes. Orchestrator also allows integration with other management and administration solutions through its open plug-in architecture.

LCM Compatibility with vCenter Server

LCM 1.2 works with vCenter Server 4.1 and vCenter Server 4.0 Update 2.

Before you install LCM, make sure that you have a compatible version of vCenter Server installed.

Lifecycle Manager Components

You must configure the required components for LCM to function properly.

Service directory	Defines which users can connect to LCM, and also defines their permission levels. Only users who are members of a directory group can log in.
Database	Stores all information that is related to LCM, such as virtual machine names, control groups, view groups, commission and decommission dates, infrastructure elements linked with the virtual machine request (such as template profile, datastore, resource pool, and so on). The information necessary to map criteria and the infrastructure is also stored in the database.
vCenter Server	Responsible for all communication with VMware vCenter Server. A Web Service API is used to connect to vCenter Server.

The components shown in Figure 1-2 must be configured in the Orchestrator configuration interface.

Figure 1-2. Architecture of LCM and Orchestrator
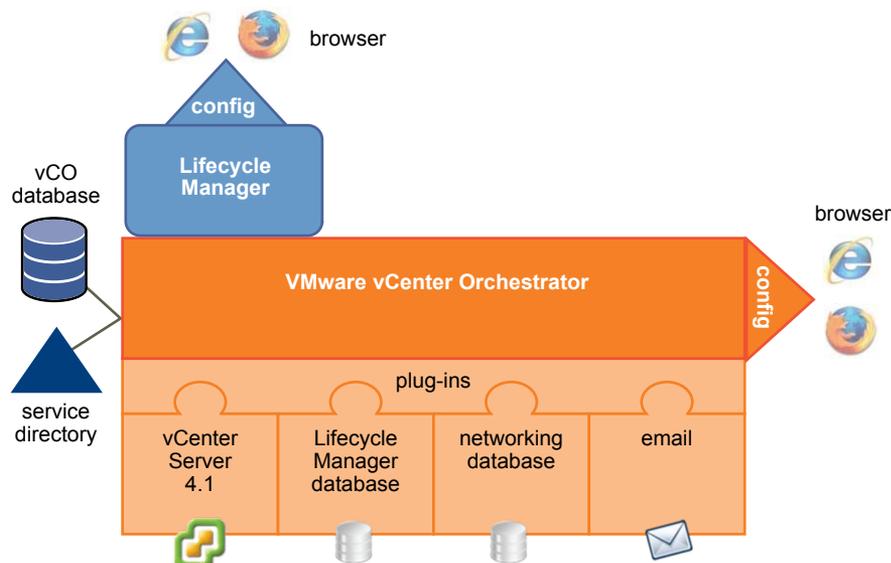
Orchestrator Plug-Ins

After you install LCM, you must configure the following Orchestrator plug-ins:

- **vCenter Server 4.1**

  For adding vCenter Server instances.

- **vCenter Lifecycle Manager**

  For configuring the Lifecycle Manager database.

- **Networking**

  For configuring the networking database.

- **Mail**

  For configuring email notifications.

LCM Installation Process

2

You must install and configure LCM by using both the Orchestrator configuration interface and the LCM interface.

Before installing LCM, you must install and configure vCenter Orchestrator. You must use the Orchestrator configuration interface to configure the components that are related to the engine, such as the database, network, server certificate, and so on. These components must be configured correctly so that LCM functions properly.

Table 2-1 lists the interfaces that you must use to complete the installation process.

Table 2-1. LCM Installation Interfaces

Installation Task	Installation Interface
Install and configure Orchestrator	Orchestrator configuration interface
Install LCM and configure LCM plug-ins	Orchestrator configuration interface
Configure LCM	LCM interface

NOTE LCM 1.1.x users can upgrade to LCM 1.2. If you want to upgrade your LCM 1.1.x and Orchestrator 4.0.1 installation, see Chapter 11, "Upgrading to Orchestrator 4.1 and LCM 1.2," on page 75, before proceeding with the installation.

System Requirements 3

Your system must meet the technical requirements that are necessary to install and configure VMware vCenter Orchestrator and VMware vCenter Lifecycle Manager. Because LCM runs as an Orchestrator plug-in, the hardware requirements and the supported operating systems are the same for both products.

This chapter includes the following topics:

- "Hardware Requirements for Orchestrator," on page 19
- "Operating Systems Supported by Orchestrator," on page 19
- "Supported Directory Services," on page 20
- "Supported Browsers," on page 20
- "Database Requirements," on page 20

Hardware Requirements for Orchestrator

Make sure your system meets the minimum hardware requirements before you install Orchestrator.

- 2.0GHz or faster Intel or AMD x86 processor. At least two CPUs are recommended. Processor requirements might differ if your database runs on the same hardware.
- 4GB RAM. You might need more RAM if your database runs on the same hardware.
- 2GB disk space. You might need more storage if your database runs on the same hardware.
- A free static IP address.

Operating Systems Supported by Orchestrator

Orchestrator offers support for several operating systems.

- Windows Server 2008 Enterprise, 64-bit
- Windows Server 2008 Standard, 64-bit
- Windows Server 2008 R2 Datacenter, 64-bit
- Windows Server 2008 R2 Enterprise, 64-bit
- Windows Server 2008 R2 Standard, 64-bit

Supported Directory Services

LCM requires a working LDAP server on your infrastructure.

LCM supports these directory service types.

- Windows Server 2003 Active Directory

- Windows Server 2008 Active Directory

- Sun Java Directory Server Enterprise Edition (DSEE) Version 6.3

Supported Browsers

The LCM user interface requires a Web browser.

You must use one of the following browsers to connect to LCM.

- Microsoft Internet Explorer 6, 7, or 8

- Mozilla Firefox 3.0.19 or 3.6.x

To connect to a virtual machine through your browser, you must use the VMware WebCenter Remote MKS Plug-in, which is compatible with the following browsers and operating systems:

- Microsoft Internet Explorer 6 or 7 on Windows XP or Windows Server 2003

- Mozilla Firefox 3.0.19 or 3.6.x on Windows XP, Windows Server 2003, Windows Server 2008, Windows 7, or Linux

Database Requirements

Orchestrator requires you to have a database that is separate from the standard vCenter database.

LCM can use either the same database as Orchestrator or a separate database. The best practice is to use a separate database for LCM.

NOTE Because of CPU and memory use, you should consider hosting the database and the Orchestrator server on different machines from the same datacenter. Make sure at least 1GB of free disk space is available on each machine.

The following database types are supported by LCM.

- Microsoft SQL Server 2005 Service Pack 2 x64

- Microsoft SQL Server 2008 Enterprise Edition x64 (10.0.1600)

- Oracle 10g Standard Edition, Release 2 (10.2.0.3.0)

- Oracle 11g Standard Edition, Release 1 x64 (11.1.0.7.0)

Installing and Configuring Orchestrator

Orchestrator Components Setup Guidelines

4

To enhance the availability and scalability of your Orchestrator setup, install Orchestrator on a server different from the server on which vCenter Server runs. Separating Orchestrator from vCenter Server makes it possible to adjust the operating system to meet the specific recommendations for each service.

This chapter includes the following topics:

vCenter Server Setup

Increasing the number of vCenter Server instances causes Orchestrator to manage more sessions. Each active session implies activity on the corresponding vCenter and too many active sessions can cause Orchestrator to experience timeouts when more than 10 vCenter connections occur.

NOTE   Run only one vCenter Server on a virtual machine. You can run multiple vCenter instances on different virtual machines in your Orchestrator setup if your network has sufficient bandwidth and latency. If you are using LAN to improve the communication between Orchestrator and vCenter, a 100Mb line is mandatory.

Directory Services Setup

Orchestrator requires a connection to an LDAP server on your infrastructure.

The supported directory service types are Active Directory and Sun Java System Directory Server.

Connect your system to the LDAP server that is physically closest to your Orchestrator server and avoid connections to remote LDAP servers. Long response times for LDAP queries can lead to slower performance of the whole system.

To improve the performance of the LDAP queries, keep the user and group lookup base as narrow as possible. Try to limit the users to targeted groups that are going to need access, rather than to whole organizations with many users who are not going to need access. Depending on the combination of database and directory service you choose, the resources you need can vary. For recommendations, see third-party documentation.

Orchestrator Database Setup

Orchestrator requires a database to store workflows and actions.

The supported database types are Oracle and Microsoft SQL Server.

The way in which your database is set up can affect Orchestrator performance. Install the database on a virtual machine other than the one on which Orchestrator is installed. This method avoids the JVM and DB server having to share CPU, RAM, and IOs.

Storing your database plug-ins in a database separate from the one that Orchestrator uses allows more modularity when upgrading the system. A dedicated database instance allows you to perform upgrades and maintenance without impacting other products.

The location of the database is important because almost every activity on the Orchestrator server triggers operations on the database. To avoid latency in the database connection, connect to the database server that is closest to your Orchestrator server and that is on the network with the highest bandwidth.

The size of the Orchestrator database varies depending on the setup and how workflow tokens are handled. Allow for approximately 50K per vCenter Server object and 4KB per workflow run.

CAUTION Make sure that at least 1GB of free disk space is available

■ on the virtual machine where the database is installed

■ on the virtual machine where the Orchestrator server is installed

Insufficient disk storage space might result in unwanted behavior of the Orchestrator server and client.

Orchestrator Configuration Maximums

When you configure Orchestrator, make sure you stay at or below the supported maximums.

Table 4-1 contains information about the tested and recommended configuration maximums for Orchestrator.

Table 4-1. Orchestrator Configuration Maximums

Item	Maximum
Connected vCenter Server systems	10
Connected ESX/ESXi servers	100
Connected virtual machines	3000
Concurrent running workflows	150

Install Orchestrator

<div style="text-align: right; font-size: 3em;">5</div>

You can install vCenter Orchestrator 4.1 only on a 64-bit operating system platform. If you run the installer in a 32-bit environment, the installation quits with a message stating that there was an error loading the Java VM.

In production environments, and to enhance the scalability of your vCenter Orchestrator setup, install Orchestrator on a dedicated Microsoft Windows server.

Prerequisites

Make sure that your hardware meets the Orchestrator system requirements. See "Hardware Requirements for Orchestrator," on page 19.

Procedure

1   Download the vCenter Orchestrator installer from the vCenter Lifecycle Manager download page.

2   Double-click the executable file and click **Next**.

3   Select **I accept the terms of the License Agreement** and click **Next**.

4   Select the Orchestrator installation directory.

Option	Action
Accept the default location	Click **Next** to accept the default installation directory `C:\Program Files\VMware\Orchestrator`.
Select a different location	Browse for a different installation directory and click **Next**.

⚠️ **CAUTION**   You cannot install Orchestrator in a directory whose name contains non-ASCII characters. If you are operating in a locale that features non-ACSII characters, you must install Orchestrator in the default location. This is due to a third-party limitation.

5   Select the type of installation and click **Next**.

Option	Description
Client	Installs the Orchestrator client application, which allows you to create and edit workflows.
Server	Installs the Orchestrator platform.
Client-Server	Installs the Orchestrator client and server.

6   Specify the location for the Orchestrator shortcuts and click **Next**.

⚠️ **CAUTION**   The name of the shortcuts directory must not contain non-ASCII characters.

7   Click **Install** to complete the installation process.

8   Click **Done** to close the installer.

What to do next

Check the status of the configuration service and start it if necessary. See "Check Configuration Readiness," on page 28.

Configuring Orchestrator 6

You must use the Orchestrator Web Configuration tool to configure the components that are related to the Orchestrator engine, such as network, database, server certificate, and so on. The correct configuration of these components ensures the proper functioning of Lifecycle Manager or any other applications running on the Orchestrator platform.

This chapter includes the following topics:

Check Configuration Readiness

Before you start configuring Orchestrator, you can check whether the Web configuration service is ready.

Procedure

1   In Windows, select **Start > Programs > Administrative Tools > Services**.

2   Select **VMware vCenter Orchestrator Configuration**.

3   If the status is not Started, right-click **VMware vCenter Orchestrator Configuration** and select **Start**.

Log In to the Orchestrator Configuration Interface

To start the configuration process, you must access the Orchestrator configuration interface.

Prerequisites

The VMware vCenter Orchestrator Configuration service must be running.

⚠ CAUTION   To avoid potential exploitation of the administrative credentials, change the nonsecure password when you first access the configuration interface. Retaining the default password might cause serious security issues in a production environment and is a common cause of data breach.

Procedure

1   Select **Start > Programs > VMware > vCenter Orchestrator Web Configuration**.

You can also access the Orchestrator configuration interface by entering the following URL address in a Web browser:

`http://orchestrator_server_DNS_name_or_IP_address:8282`

8282 is the default HTTP access port reserved for the Web UI of Orchestrator configuration. To enable HTTPS connection through port 8283, you must configure Jetty to use SSL. See *Jetty Documentation, Configuring SSL*.

2   Log in with the default credentials.

■   User name: `vmware`.

You cannot change the `vmware` default user name.

■   Password: `vmware`

When you log in to the Orchestrator configuration interface for the first time, you see the installation path, the Orchestrator version, and the server status in the **Information** tab. The status indicators of all tabs on the left display red triangles, indicating that the components are not configured.

What to do next

Select a tab and follow the links in the inspector on the right, entering the necessary information until a green circle appears on the selected tab. The green circle indicates that your configuration changes are correct and that all dependencies are met.

Change the Default Password

You must change the default password to avoid potential security issues.

Prerequisites

The VMware vCenter Orchestrator Configuration service must be running.

> ⚠️ **CAUTION** To avoid potential exploitation of the administrative credentials, change the nonsecure password when you first access the configuration interface. Retaining the default password might cause serious security issues in a production environment and is a common cause of data breach.

Procedure

1 Log in to the Orchestrator configuration interface as `vmware`.

2 On the **General** tab, click **Change Password**.

3 In the **Current password** text box, enter `vmware`.

4 In the **New password** text box, enter the new password.

5 Reenter the new password to confirm it.

6 Click **Apply changes**.

Revert to the Default Password for Orchestrator Configuration

If the default password for the Orchestrator configuration interface is changed, you cannot retrieve it because Orchestrator uses encryption to encode passwords. You can revert to the default password vmware if the current password is not known.

Procedure

1 Navigate to the following folder on the Orchestrator server system.

   `install_directory\VMware\Orchestrator\configuration\jetty\etc`

2 Open the `password.properties` file in a text editor.

3 Delete the content of the file.

4 Add the following line to the `password.properties` file.

   `vmware=92963abd36c896b93a36b8e296ff3387`

5 Save the `password.properties` file.

6 Restart the Orchestrator Configuration service.

You can log in to the Orchestrator configuration interface with the default credentials.

- User name: `vmware`

- Password: `vmware`

Configure the Network Connection

When you install Orchestrator, the IP address for your server is set as not set. To change this, you must configure the network settings used by Orchestrator.

Prerequisites

System administrators must make sure that the network provides a fixed IP, which is obtained by using a properly configured DHCP server (using reservations) or by setting a static IP. The Orchestrator server requires that this IP address remain constant while it is running.

Procedure

1   Log in to the Orchestrator configuration interface as `vmware`.

2   Click **Network**.

3   From the **IP address** drop-down menu, select the network interface to which to bind the Orchestrator server.

    Orchestrator discovers the IP address of the machine on which the server is installed.

    When an interface is selected, the corresponding DNS name appears. If no network name is found, the IP address appears in the **DNS name** text box. Use this IP address to log in to the Orchestrator client interface.

4   Set up the communication ports.

    For more information about default ports, see "Orchestrator Network Ports," on page 30.

5   Click **Apply changes**.

What to do next

Click **SSL Certificate** to load the vCenter SSL certificate in Orchestrator.

Orchestrator Network Ports

Orchestrator uses specific ports that allow communication with the other systems. Some of the communication ports you must set are a subset of the standard ports that JBoss uses. The ports are set with a default value, but you can change these values at any time. When you make the changes, make sure that all ports are free on your host and, if necessary, open these ports on required firewalls.

Default Configuration Ports

Table 6-1 lists the default ports that Orchestrator needs to provide the Orchestrator service. You must configure your firewall to allow incoming TCP connections.

NOTE   Other ports might be required if you are using custom plug-ins.

Table 6-1. VMware vCenter Orchestrator Default Configuration Ports

Port	Number	Protocol	Source	Target	Description
Lookup port	8230	TCP	vCO Client	vCO Server	The main port to communicate with the Orchestrator server (JNDI port). All other ports communicate with the Orchestrator smart client through this port. It is part of the Jboss Application server infrastructure.
Command port	8240	TCP	vCO Client	vCO Server	The application communication port (RMI container port) used to load remotely. It is part of the Jboss Application server infrastructure.
Messaging port	8250	TCP	vCO Client	vCO Server	The Java messaging port used to dispatch events. It is part of the Jboss Application server infrastructure.

Table 6-1. VMware vCenter Orchestrator Default Configuration Ports (Continued)

Port	Number	Protocol	Source	Target	Description
Data port	8244	TCP	vCO Client	vCO Server	The port used to access all Orchestrator data models, such as workflows and policies. It is part of the Jboss Application server infrastructure.
HTTP server port	8280	TCP	end-user Web browser	vCO Server	The port used by the Orchestrator Server to connect to the Web frontend through HTTP.
HTTPS server port	8281	TCP	end-user Web browser	vCO Server	The SSL secured HTTP protocol used to connect to the Web frontend and to communicate with the vCenter API.
Web configuration HTTP access port	8282	TCP	end-user Web browser	vCO Configuration	The access port for the Web UI of Orchestrator configuration.
Web configuration HTTPS access port	8283	TCP	end-user Web browser	vCO Configuration	The SSL access port for the Web UI of Orchestrator configuration. **NOTE** To enable the HTTPS connection, configure Jetty to use SSL. See *Jetty Documentation, Configuring SSL*.

External Communication Ports

Table 6-2 lists the ports to which Orchestrator connects to communicate with external services. You must allow your firewall to allow outgoing connections.

Table 6-2. VMware vCenter Orchestrator External Communication Ports

Port	Number	Protocol	Source	Target	Description
LDAP	389	TCP	vCO Server	LDAP Server	The look up port of your LDAP Authentication server.
LDAP using SSL	636	TCP	vCO Server	LDAP Server	The look up port of your secure LDAP Authentication server.
LDAP using Global Catalog	3268	TCP	vCO Server	Global Catalog Server	The port to which Microsoft Global Catalog server queries are directed.
SQL Server	1433	TCP	vCO Server	Microsoft SQL Server	The port used to communicate with the Microsoft SQL Server that is configured as the Orchestrator database.
Oracle	1521	TCP	vCO Server	Oracle DB Server	The port used to communicate with the Oracle Database Server that is configured as the Orchestrator database.
SMTP Server port	25	TCP	vCO Server	SMTP Server	The port used for email notifications.
vCenter API port	443	TCP	vCO Server	vCenter Server	The vCenter API communication port used by Orchestrator to obtain virtual infrastructure and virtual machine information from orchestrated vCenter Server(s).

Internal JBoss Ports

Table 6-3 lists the internal JBoss Server ports. These ports do not need to be added to the firewall exceptions.

Table 6-3. Internal JBoss Server Ports

Port Number	Description
3455	RMI server registry invoker
3873	EJB3/AOP remoting connector

Table 6-3. Internal JBoss Server Ports (Continued)

Port Number	Description
4445	JBoss pooled invoker
4446	Remoting server service connector
8083	Dynamic class/resource loader

Change the Default Configuration Ports on the Orchestrator Client Side

When you change the default network ports in the Orchestrator configuration interface, your changes are applied only on the Orchestrator server side. To connect to the server with the client, you must change the configuration of all Orchestrator client instances or connect to the server by using your Orchestrator server DNS name or IP address followed by the new Lookup port number.

The main port to communicate with the Orchestrator server is the Lookup port. The Orchestrator client discovers all other ports through this port. If you change the default lookup port value in the Orchestrator configuration interface after you install the Orchestrator client instances, you can add a `vmo.properties` configuration file for each Orchestrator client instance and define the new Lookup port by adding the `ch.dunes.net.jboss-server.port` system property.

Prerequisites

Log in to the server where the vCenter Orchestrator Client application is installed.

Procedure

1   Navigate to the `apps` folder on the Orchestrator client system.

    `install_directory\VMware\Orchestrator\apps`

2   Create a file that contains the lookup port value.

    `ch.dunes.net.jboss-server.port=new_lookup_port_number`

3   Save the file as `vmo.properties`.

4   Repeat the procedure for every Orchestrator client instance.

You can log in to the Orchestrator client without adding the lookup port number to the Orchestrator server DNS name or IP address.

Import the vCenter SSL Certificate

The Orchestrator configuration interface uses a secure connection to communicate with vCenter. You can import the required SSL certificate from a URL or file.

Procedure

1   Log in to the Orchestrator configuration interface as **vmware**.

2   Click **Network**.

3   In the right pane, click the **SSL Certificate** tab.

4   Load the vCenter SSL certificate in Orchestrator from a URL address or file.

Option	Description
Import from URL	Enter URL of the vCenter server: `https://`*`your_vcenter_server_IP_address`*
Import from file	Obtain the server certificate file. Usual locations are: ■ `C:\Documents and Settings\AllUsers\ApplicationData\VMware` `\VMware VirtualCenter\SSL\rui.crt` ■ `/etc/vmware/ssl/rui.crt`

5   Click **Import**.

     A message confirming that the import is successful appears.

6   Repeat the steps for each vCenter server.

7   Click **Startup Options**.

8   Click **Restart the vCO configuration server** to restart the Orchestrator Configuration service after adding a new SSL certificate.

The imported certificate appears in the Imported SSL certificates list. On the **Network** tab, the red triangle changes to a green circle to indicate that the component is now configured correctly.

What to do next

Each time you want to specify the use of an SSL connection, you must return to the **SSL Certificate** tab on the **Network** tab and import the corresponding vCenter SSL certificate.

Configuring LDAP Settings

Orchestrator requires a connection to a working LDAP server on your infrastructure.

■   Generate the LDAP Connection URL on page 34

    The LDAP service provider uses a URL address to configure the connection to the directory server. To generate the LDAP connection URL, you must specify the LDAP host, port, and root.

■   Import the LDAP Server SSL Certificate on page 35

    If your LDAP server uses SSL, you can import the SSL certificate file to the Orchestrator configuration interface and activate secure connection between Orchestrator and LDAP.

■   Specify the Browsing Credentials on page 36

    Orchestrator must read your LDAP structure to inherit its properties. You can specify the credentials that Orchestrator uses to connect to an LDAP server.

■   Define the LDAP Lookup Paths on page 36

    You can define the users and groups lookup information.

■   Define the LDAP Search Options on page 37

    You can customize the LDAP search queries and make searching in LDAP more effective.

■   Common Active Directory LDAP Errors on page 38

    When you encounter the `LDAP:error code 49` error message and experience problems connecting to your LDAP authentication server, you can check which LDAP function is causing the problem.

Generate the LDAP Connection URL

The LDAP service provider uses a URL address to configure the connection to the directory server. To generate the LDAP connection URL, you must specify the LDAP host, port, and root.

The supported directory service types are Active Directory and Sun Java System Directory Server.

Procedure

1 Log in to the Orchestrator configuration interface as `vmware`.

2 Click **LDAP**.

3 From the **LDAP client** drop-down menu, select the directory server type that you are using as the LDAP server.

> NOTE   If you change the LDAP server or type after you set permissions on Orchestrator objects (such as access rights on workflows or actions), you must reset these permissions.
>
> If you change the LDAP settings after configuring custom applications that capture and store user information, the LDAP authentication records created in the database become invalid when used against the new LDAP database.

4 (Optional) If you use Sun Java System Directory Server you must set `objectClass` to `groupOfUniqueNames` when you add users, create groups, or assign group memberships. The User ID (`uid`) attribute is mandatory for every user that can log in to Orchestrator.

Use Java System Directory Service Control Center from Sun Microsystems to set `objectClass` to `groupOfUniqueNames`. When creating a new group, select **Entry Type > Static Group > groupOfUniqueNames** in Java System Directory Service Control Center.

5 In the **Primary LDAP host** text box, type the IP address or the DNS name of the host on which your primary LDAP service runs.

This is the first host on which the Orchestrator configuration interface verifies user credentials.

6 (Optional) In the **Secondary LDAP host** text box, type the IP address or the DNS name of the host on which your secondary LDAP service runs.

If the primary LDAP host becomes unavailable, Orchestrator verifies user credentials on the secondary host.

7 In the **Port** text box, type the value for the look up port of your LDAP server.

> NOTE   Orchestrator supports Active Directory hierarchical domains structure. If your Domain Controller is configured to use Global Catalog, you must use port 3268. You cannot use the default port 389 to connect to the Global Catalog server.

8 In the **Root** text box, type the root element of your LDAP service.

If your domain name is company.org, your root LDAP is `dc=company,dc=org`.

This is the node used to browse your service directory after typing the appropriate credentials. For large service directories, specifying a node in the tree narrows the search and improves performance. For example, rather than searching in the entire directory, you can specify `ou=employees,dc=company,dc=org`. This displays all the users in the Employees group.

9 (Optional) Select the **Use SSL** check box to activate encrypted certification for the connection between Orchestrator and LDAP.

If your LDAP uses SSL, you must first import the SSL certificate and restart the Orchestrator Configuration service. See "Import the LDAP Server SSL Certificate," on page 35.

10 (Optional) Select the **Use Global Catalog** check box to allow LDAP referrals when the LDAP client is Active Directory.

The LDAP server look up port number changes to 3268. Orchestrator follows the LDAP referrals to find users and groups in a subdomain that is part of the Active Directory tree to which Orchestrator is connected. You can add permissions on any groups that can be accessed from your Global Catalog.

Example 6-1. Example Values and Resulting LDAP Connection URL Addresses

- LDAP host: `DomainController`

- Port: `389`

- Root: `ou=employees,dc=company,dc=org`

Connection URL: `ldap://DomainController:389/ou=employees,dc=company,dc=org`

- LDAP host using Global Catalog: `10.23.90.130`

- Port: `3268`

- Root: `dc=company,dc=org`

Connection URL: `ldap://10.23.90.130:3268/dc=company,dc=org`

What to do next

Assign credentials to Orchestrator to ensure its access to the LDAP server. See "Specify the Browsing Credentials," on page 36.

Import the LDAP Server SSL Certificate

If your LDAP server uses SSL, you can import the SSL certificate file to the Orchestrator configuration interface and activate secure connection between Orchestrator and LDAP.

SSL capabilities are not installed as part of Microsoft Active Directory and Sun Java Directory Server, and require more configuration. For instructions about configuring your LDAP server for SSL access, see third-party documentation.

Prerequisites

- Verify that SSL access is enabled on the LDAP server.

- Obtain a self-signed server certificate or a certificate that is signed by a Certificate Authority.

Procedure

1 Log in to the Orchestrator configuration interface as `vmware`.

2 Click **Network**.

3 In the right pane, click the **SSL Certificate** tab.

4 Browse to select a certificate file to import.

5 Click **Import**.

A message confirming that the import is successful appears.

6   Click **Startup Options**.

7   Click **Restart the vCO configuration server** to restart the Orchestrator Configuration service after adding a new SSL certificate.

The imported certificate appears in the Imported SSL certificates list. You activated secure connection between Orchestrator and your LDAP server.

What to do next

You must enable SSL on the **LDAP** tab in the Orchestrator configuration interface.

Specify the Browsing Credentials

Orchestrator must read your LDAP structure to inherit its properties. You can specify the credentials that Orchestrator uses to connect to an LDAP server.

Prerequisites

You must have a working LDAP service on your infrastructure and have generated the LDAP connection URL.

Procedure

1   In the **LDAP** tab of the Orchestrator configuration interface, enter a valid user name (LDAP string) in the **User name** text box for a user on your LDAP who has browsing permissions.

The possible formats in which you can specify the user name in Active Directory are as follows:

■   Bare user name format, for example `user`.

■   Distinguished name format: `cn=user,ou=employees,dc=company,dc=org`.

Use this format with OpenLDAP and Sun. No spaces between the comma and the next identifier.

■   Principle name format: `user@company.org`.

■   NetBEUI format: `COMPANY\user`.

2   In the **Password** text box, enter the valid password for the user name you entered in Step 1.

Orchestrator uses these credentials to connect to the LDAP server.

What to do next

Define the LDAP containers for Orchestrator to look up users and groups.

Define the LDAP Lookup Paths

You can define the users and groups lookup information.

Two global roles are identified in Orchestrator: Developers and Administrators. The users in the Developers role have editing privileges on all elements. The users in the Administrators role have unrestricted privileges. Administrators can manage permissions, or discharge administration duties on a selected set of elements to any other group or user. These two groups must be contained in the Group lookup base.

Prerequisites

You must have a working LDAP service on your infrastructure.

Procedure

1   Log in to the Orchestrator configuration interface as `vmware`.

2   Click **LDAP**.

3   Define the **User lookup base**.

This is the LDAP container (the top level domain name or organizational unit) where Orchestrator searches for potential users.

a   Click **Search** and type the top-level domain name or organizational unit.

Searching for `company` returns `dc=company,dc=org` and other common names containing the search term. If you type `dc=company,dc=org` as a search term, no results are found.

b   Click the LDAP connection string for the discovered branch to insert it in the **User lookup base** text box.

If no matches are found, check your LDAP connection string in the main LDAP page.

NOTE   You can connect to the Global Catalog Server through port 3268. It issues LDAP referrals which Orchestrator follows to find the account or group in a subdomain.

4   Define the **Group lookup base**.

This is the LDAP container where Orchestrator looks up groups.

a   Click **Search** and type the top-level domain name or organizational unit.

b   Click the LDAP string for the discovered branch to insert it in the **Group lookup base** text box.

5   Define the **vCO Admin group**.

This must be an LDAP group (like Domain Users) to which you grant administrative privileges for Orchestrator.

a   Click **Search** and type the top-level group name.

b   Click the LDAP string for the discovered branch to insert it in the **vCO Admin group** text box.

6   Click the **Test Login** tab and type credentials for a user to test whether they can access the Orchestrator smart client.

After a successful login, the system checks if the user is in the Orchestrator Administrator group.

What to do next

Define the LDAP search options and apply your changes.

Define the LDAP Search Options

You can customize the LDAP search queries and make searching in LDAP more effective.

Procedure

1   Log in to the Orchestrator configuration interface as `vmware`.

2   Click **LDAP**.

3   In the **Request timeout** text box, enter a value in milliseconds.

This value determines the period during which the Orchestrator server sends a query to the service directory, the directory searches, and sends a reply. If the timeout period elapses, modify this value to check whether the timeout occurs in the Orchestrator server.

4   (Optional) For all links to be followed before the search operation is performed, select the **Dereference links** check box.

Sun Java System Directory Server does not support reference links. If you are using it, you must select the **Dereference links** check box.

5   (Optional) To filter the attributes that the search returns, select the **Filter attributes** check box.

Selecting this check box makes searching in LDAP faster. However, you might need to use some extra LDAP attributes for automation later.

6   (Optional) Select the **Ignore referrals** check box to disable referral handling.

When you select the check box, the system does not display any referrals.

7   In the **Host reachable timeout** text box, enter a value in milliseconds.

This value determines the timeout period for the test checking the status of the destination host.

8   Click **Apply changes**.

On the **LDAP** tab, the red triangle changes to a green circle to indicate that the component is now configured correctly.

What to do next

Proceed with the database configuration.

Common Active Directory LDAP Errors

When you encounter the `LDAP:error code 49` error message and experience problems connecting to your LDAP authentication server, you can check which LDAP function is causing the problem.

Table 6-4 lists the most common Active Directory LDAP authentication errors.

Table 6-4. Common Active Directory LDAP Errors

Error	Description
525	The user is not found.
52e	The user credentials are not valid.
530	The user is not allowed to log in at this time.
531	The user is not allowed to log in to this workstation.
532	The password has expired.
533	This user account has been disabled.
701	This user account has expired.
773	The user must reset their password.
775	The user account has been locked.

Password Encryption and Hashing Mechanism

Orchestrator utilizes PBE with MD5 and DES encryption mechanism to encode the stored passwords used to connect to the database, LDAP, and Orchestrator servers.

Table 6-5 shows the password encryption and hashing mechanisms used by Orchestrator.

Table 6-5. Encryption and Hashing Algorithms

Algorithm	Description
Password Based Encryption (part of Java 2 SDK 1.4)	Generates an encryption key from a password. PBE stores and checks the hash value of the password. For more information, see the *Java Cryptography Extension Reference Guide* on java.sun.com.
Message Digest 5 algorithm	Generates a 128-bit cryptographic message digest value, usually expressed as a 32 digit hexadecimal number.
Data Encryption Standard	Applies a 56-bit key to each 64-bit block of data.

Configure the Database Connection

To establish a connection to the Orchestrator database, you must configure the database connection parameters.

Prerequisites

- Set up a new database to use with the Orchestrator server. See "Orchestrator Database Setup," on page 23.

- For a list of database connection parameters, see "Database Connection Parameters," on page 40.

- If you are using an SQL Server database, verify that the SQL Server Browser service is running.

- To store characters in the correct format in an Oracle database, set the NLS_CHARACTER_SET parameter to AL32UTF8 before configuring the database connection and building the table structure for Orchestrator. This setting is crucial for an internationalized environment.

Procedure

1 Log in to the Orchestrator configuration interface as **vmware**.

2 Click **Database**.

3 From the **Select the database type** drop-down menu, select the type of database for Orchestrator server to use.

NOTE   LCM supports Oracle and SQL Server databases.

4 Specify the database connection parameters.

If the specified parameters are correct, a message states that the connection to the database is successful.

NOTE   Although Orchestrator has established a connection to the database, the database configuration is not yet complete. You must install or update the database.

5   To build or update the table structure for Orchestrator, install or update the database.

Option	Description
Install the database	Configures a new database.
Update the database	Uses the database from your previous Orchestrator installation.

After the database is populated, you can reset the database access rights to **db_dataread** and **db_datawrite**.

6   Click **Apply changes**.

NOTE   If you change the Orchestrator database after configuring and installing the default plug-ins, click the **Troubleshooting** tab and force plug-in reinstallation by clicking the **Reset current version** link. This operation deletes the *install_directory*\app-server\server\vmo\plugins _VSOPluginInstallationVersion.xml file, which holds the version of the plug-ins already installed, and forces plug-in reinstallation.

The database configuration is successfully updated. On the **Database** tab, the red triangle changes to a green circle to indicate that the component is now configured correctly.

Database Connection Parameters

To establish a connection to the database, you must specify the database connection parameters. Depending on the type of database you are connecting to, the required information may vary.

Table 6-6 lists the connection parameters that you must specify.

Table 6-6. Database Connection Parameters

Connection Parameter	Description
User name	The user name that Orchestrator uses to connect and operate the selected database. The name you select must be a valid user on the target database with db_owner rights.
Password	The valid password for the user name you entered.
Database host IP address or DNS name	The database server IP address or DNS name.
Port	The database server port that allows communication to your database.
Database name	The full unique name of your database. The database name is specified by the SERVICE_NAMES parameter in the initialization parameter file.
Instance name	The name of the database instance that can be identified by the INSTANCE_NAME parameter in the database initialization parameter file.
Domain (SQL Server only)	To use Windows authentication, enter the Windows domain, for example **company.org**. To use SQL authentication, leave this text box blank.
Use Windows authentication mode (SQL Server only)	Select to send NTLMv2 responses when using Windows authentication.

Identify the SQL Server Authentication Type

You can identify whether SQL Server is using Windows NT or SQL Server authentication.

Procedure

1   Open the SQL Server Management Studio.

2   Click the **Properties** tab.

3   Check the connection type.

Server Certificate

The server certificate is a form of digital identification that is used with HTTPS to authenticate Web applications. Issued for a particular server and containing information about the server's public key, the certificate allows you to sign all elements created in Orchestrator and guarantee authenticity. When the client receives an element from your server (typically this is a package), they verify your identity and decide whether to trust your signature.

- Import a Server Certificate on page 41

  You can import a server certificate and use it with Orchestrator.

- Create a Self-Signed Server Certificate on page 42

  Installing Orchestrator requires that you create a self-signed certificate. You can create a self-signed certificate to guarantee encrypted communication and a signature for your packages. However, the recipient cannot be sure that the self-signed package you are sending is in fact a package issued by your server and not a third party claiming to be you.

- Obtain a Server Certificate Signed by a Certificate Authority on page 42

  To provide recipients with an acceptable level of trust that the package was created by your server, certificates are typically signed by a Certificate Authority (CA). Certificate Authorities guarantee that you are who you claim to be, and as a token of their verification, they sign your certificate with their own.

- Export a Server Certificate on page 43

  The server certificate private key is stored in the vmo_keystore table of the Orchestrator database. In case you lose or delete this key, or if you bind the Orchestrator server to a different database, the content of the exported packages signed with this certificate will become unavailable. To ensure that packages are decrypted on import, you must save this key to a local file.

- Change a Self-Signed Server Certificate on page 43

  If you want to sign your packages with a server certificate different from the one you used for the initial Orchestrator configuration, you need to export all your packages and reinstall the Orchestrator server.

Import a Server Certificate

You can import a server certificate and use it with Orchestrator.

Procedure

1 Log in to the Orchestrator configuration interface as `vmware`.

2 Click **Server Certificate**.

3 Click **Import certificate database**.

4 Browse to select the certificate file to import.

5 Enter the password used to decrypt the content of the imported keystore database.

The details about the imported server certificate appear in the Server Certificate window.

Create a Self-Signed Server Certificate

Installing Orchestrator requires that you create a self-signed certificate. You can create a self-signed certificate to guarantee encrypted communication and a signature for your packages. However, the recipient cannot be sure that the self-signed package you are sending is in fact a package issued by your server and not a third party claiming to be you.

Procedure

1   Log in to the Orchestrator configuration interface as `vmware`.

2   Click **Server Certificate**.

3   Click **Create certificate database and self-signed server certificate**.

4   Enter the relevant information.

5   From the drop-down menu, select a country.

6   Click **Create**.

Orchestrator generates a server certificate that is unique to your environment. The details about the certificate public key appear in the Server Certificate window. The certificate private key is stored in the `vmo_keystore` table of the Orchestrator database.

What to do next

For disaster recovery purposes, you can save the certificate private key to a local file.

Obtain a Server Certificate Signed by a Certificate Authority

To provide recipients with an acceptable level of trust that the package was created by your server, certificates are typically signed by a Certificate Authority (CA). Certificate Authorities guarantee that you are who you claim to be, and as a token of their verification, they sign your certificate with their own.

Prerequisites

Create a self-signed server certificate or import an existing server certificate.

Procedure

1   Log in to the Orchestrator configuration interface as `vmware`.

2   Click **Server Certificate**.

3   Generate a Certificate Signing Request (CSR).

    a   Click **Export certificate signing request**.

    b   Save the `VSOcertificate.csr` file in your file system when prompted.

4   Send the CSR file to a Certificate Authority, such as Verisign or Thawte.

    Procedures might vary from one CA to another, but they all require a valid proof of your identity.

    CA returns a Certificate Signing Request that you must import. This is an exact copy of your actual certificate and the CA signature.

5   Click **Import certificate signing request signed by GA** and select the file sent by your CA.

Orchestrator uses the server certificate to

■   Sign all packages before they are exported by attaching your certificate's public key to each one.

■   Display a user prompt on importing a package that contains elements signed by untrusted certificates.

What to do next

You can import this certificate on other servers.

Export a Server Certificate

The server certificate private key is stored in the vmo_keystore table of the Orchestrator database. In case you lose or delete this key, or if you bind the Orchestrator server to a different database, the content of the exported packages signed with this certificate will become unavailable. To ensure that packages are decrypted on import, you must save this key to a local file.

Prerequisites

You must have created or imported a server certificate.

Procedure

1   Log in to the Orchestrator configuration interface as `vmware`.

2   Click **Server Certificate**.

3   Click **Export certificate database**.

4   Enter a password to encrypt the content of the exported keystore database.

    You must enter this password again when importing the file.

5   Click **Export**.

6   Save the `vmo-server.vmokeystore` file when prompted.

Change a Self-Signed Server Certificate

If you want to sign your packages with a server certificate different from the one you used for the initial Orchestrator configuration, you need to export all your packages and reinstall the Orchestrator server.

Procedure

1   Export all your packages.

    a   Click the **Packages** view in the Orchestrator client.

    b   Right-click the package to export and select **Export package**.

    c   Browse to select a location in which to save the package and click **Open**.

    d   Leave the **View content**, **Re-Packageable**, and **Edit element** options selected.

    ⚠ CAUTION   Do not sign the package with your current certificate. You must not encrypt the package. When you delete the certificate database, the private key will be lost and the content of the exported package will become unavailable.

    e   (Optional) Deselect the **Export version history** check box if you do not want to export the version history.

    f   Click **Save**.

2   (Optional) Export the Orchestrator configuration.

3   Uninstall the Orchestrator server.

4   Delete the Orchestrator database, or create a backup if you want to keep old data.

    The database you bind Orchestrator to must not contain records in the vmo_keystore table.

5   Reinstall the Orchestrator server.

6　　(Optional) Import your Orchestrator configuration.

7　　Create a new self-signed certificate or import one.

8　　Reimport your packages.

    a　　Click the **Packages** view in the Orchestrator client.

    b　　From the drop-down menu, select **Import package**.

    c　　Browse to select the package to import and click **Open**.

    d　　Click **Import** or **Import and trust provider**.

    e　　Click **Import checked elements**.

The server certificate change is effective at the next package export.

Configure the Default Plug-Ins

To deploy the set of default plug-ins when the Orchestrator server starts, the system must authenticate against the LDAP server. You can specify the administrative credentials that Orchestrator uses with plug-ins, and enable as well as disable plug-ins on the **Plug-ins** tab.

If you change the Orchestrator database after configuring and installing the default plug-ins, you must click the **Reset current version** link in the **Troubleshooting** tab. This operation deletes the *install_directory*\app–server\server\vmo\plugins_VSOPluginInstallationVersion.xml file, which holds the version of the plug-ins already installed, and forces plug-in reinstallation.

Procedure

1　　Log in to the Orchestrator configuration interface as **vmware**.

2　　Click **Plug-ins**.

3　　Type the credentials for a user who is a member of the Orchestrator Administration group that you specified on the **LDAP** tab.

When the Orchestrator server starts, the system uses these credentials to set up the plug-ins. The system checks the enabled plug-ins and performs any necessary internal installations such as package import, policy run, script launch, and so on.

4　　(Optional) Install a new plug-in.

    a　　Click the magnifying glass icon.

    b　　Select the file to install.

    c　　Click **Open**.

    d　　Click **Upload and install**.

The allowed file extensions are .vmoapp and .dar. A .vmoapp file can contain a collection of several .dar files and can be installed as an application, while a .dar file contains all the resources associated with one plug-in.

The installed plug-in file is stored in the *install_directory*\app–server\server\vmo\plugins folder.

NOTE　If you add a .dar file directly to the file system, you must click **Reload plug-ins** to update the plug-ins available to the Orchestrator configuration interface.

5   (Optional) To disable a plug-in, deselect the check box next to it.

This action does not remove the plug-in file.

6   Click **Apply changes**.

On the **Plug-ins** tab, the red triangle changes to a green circle to indicate that the component is now configured correctly. The first time the server boots, it installs the selected plug-ins.

What to do next

You can now configure the settings for Mail, SSH, and vCenter 4.1 plug-ins.

Define the Default SMTP Connection

The Mail plug-in is installed with Orchestrator Server and is used for email notifications. The only option available for this plug-in is to use default values for new mail messages. You can set the default email account.

Avoid load balancers when configuring mail in Orchestrator. You will get SMTP_HOST_UNREACHABLE.

Procedure

1   Log in to the Orchestrator configuration interface as `vmware`.

2   Click **Mail**.

3   Select the **Define default values** check box and fill in the required text boxes.

Text box	Description
SMTP host	Enter the IP address or domain name of your SMTP server.
SMTP port	Enter a port number to match your SMTP configuration. The default SMTP port is 25.
User name	Enter a valid email account. This is the email account Orchestrator uses to send emails.
Password	Enter the password associated with the user name.
From name and address	Enter the sender information to appear in all emails sent by Orchestrator.

4   Click **Apply changes**.

Configure the SSH Plug-In

You can set up the SSH plug-in to ensure encrypted connections.

Procedure

1   Log in to the Orchestrator configuration interface as `vmware`.

2   Click **SSH**.

3   Click **New connection**.

4   In the **Host name** text box, enter the host to access with SSH through Orchestrator.

NOTE   The username and password are not required because Orchestrator uses the credentials of the currently logged-in user to run SSH commands. You must reproduce the accounts you want to work on SSH on target hosts from the LDAP server.

5   Click **Apply changes**.

The host is added to the list of SSH connections.

6   (Optional) Configure an entry path on the server.

    a   Click **New root folder**.

    b   Enter the new path and click **Apply changes**.

The SSH host is available in the **Inventory** view of the Orchestrator smart client.

Configure the vCenter Server 4.1 Plug-In

Orchestrator uses the vCenter Web Service API to control vCenter Server. You can set all the parameters to enable Orchestrator to connect to your vCenter Sever instances.

Prerequisites

Import the SSL certificates for each vCenter Server instance you define. For more information, see "Import the vCenter SSL Certificate," on page 32.

Procedure

1   Log in to the Orchestrator configuration interface as `vmware`.

2   Click **vCenter Server 4.1**.

3   Click **New vCenter Server Host**.

4   From the **Available** drop-down menu, select **Enabled**.

5   In the **Host** text box, type the IP address or the DNS name of the vCenter Server host.

6   In the **Port** text box, leave the default value, `443`.

7   (Optional) Select the **Secure channel** check box to establish a secure connection to your vCenter Server host.

8   In the **Path** text box, use the default value, `/sdk`.

This is the location of the SDK that you use to connect to your vCenter Server instance.

9   In the **User name** and **Password** text boxes, type the credentials for Orchestrator to use to establish the connection to the vCenter Server host.

The user that you select must be a valid user with administrative privileges on your vCenter Server, preferably at the top of the vCenter Server tree structure. Orchestrator uses these credentials to monitor the vCenter Web service (typically to operate Orchestrator system workflows). All other requests inherit the credentials of the user who triggers an action.

10   Select **Share a unique session** as the method to manage user access on the vCenter Server host, and enter the credentials of a user who is a vCenter Server administrator.

    Note   **Session per user** mode is not supported by LCM.

11   Click **Apply changes**.

The URL to the newly configured vCenter Server host is added to the list of defined hosts.

12   Repeat Step 3 through Step 11 for each vCenter Server instance.

Remove a Plug-In

You can disable an Orchestrator plug-in from the **Plug-ins** tab, but this action does not remove the plug-in file from the Orchestrator server file system. To remove the plug-in file, you must log in to the machine on which the Orchestrator server is installed and remove the plug-in file manually.

Prerequisites

Log in to the machine on which the Orchestrator server is installed.

Procedure

1   Navigate to the Orchestrator installation folder on the Orchestrator server system.

    `install_directory\VMware\Orchestrator\app-server\server\vmo\plugins`

2   Delete the `.dar` archive that contains the plug-in to remove.

3   Restart the Orchestrator Configuration service.

    The plug-in is removed from the Orchestrator configuration interface.

4   Log in to the Orchestrator client.

5   Click the **Packages** view in the Orchestrator client.

6   Right-click the package to delete and select **Delete element with content**.

    NOTE Orchestrator elements that are locked in the read-only state, for example workflows in the standard library, are not deleted.

You removed all custom workflows and actions, policies, Web views, configurations, settings, and resources that the plug-in contains.

Import the vCenter Server License

To finish the configuration of the Orchestrator server, you must import the vCenter Server license.

Prerequisites

Import the SSL certificate for the licensed vCenter Server host. See "Import the vCenter SSL Certificate," on page 32.

Procedure

1   Log in to the Orchestrator configuration interface as `vmware`.

2   Click **Licenses**.

3   On the **vCenter Server License** tab, enter the details about the vCenter Server host on which Orchestrator must verify the license key.

   a   In the **Host** text box, type the IP address or the DNS name of the vCenter Server host.

   b   In the **Port** text box, leave the default value, `443`.

   c   (Optional) Select the **Secure channel** check box to establish a secure connection to the vCenter Server host.

   d   In the **Path** text box, use the default value, `/sdk`.

       This is the location of the SDK that you use to connect to your vCenter Server instance.

   e   In the **User name** and **Password** text boxes, type the credentials for Orchestrator to use to establish the connection to vCenter.

       The user you select must be a valid user with administrative privileges on your vCenter Server, preferably at the top of the vCenter tree structure.

   To view details, click **License details**.

4   (Optional) If the version of your vCenter Server is earlier than version 4.0, you must add the license key manually.

   a   Select the **Add vCenter Server license manually** option.

   b   In the **Serial number** text box, type your vCenter Server license key.

       The serial number is a string of five hyphen-separated groups of five alphanumeric characters each.

   To view details, click the name of the imported license.

5   Click **Apply changes**.

6   Start the Orchestrator server.

The Orchestrator server is now configured correctly.

Start the Orchestrator Server

You can install the Orchestrator server as a service on the **Startup Options** tab. When you do this, you can start, stop, and restart the service from the Configuration interface. This is process is reversible as you can always use the **Uninstall vCO server from service** option.

Prerequisites

Verify that your Orchestrator system has at least 2GB of RAM. The Orchestrator server might not start if your system does not meet this requirement.

All of the status indicators must display a green circle. You cannot start the Orchestrator server if any of the components is not configured properly.

Procedure

1   Click **Startup Options**.

2   Click **Install vCO server as service**.

   The Orchestrator server is installed as a Windows service.

3   Click **Start service**.

   The Orchestrator server status appears as `Service is starting`. The first boot can take around 5-10 minutes because it is building the database tables.

A message states that the service is started successfully. The Orchestrator server status appears at the bottom of each configuration tab and is one of the following:

- Running
- Not available
- Stopped

To see the Orchestrator server status, update the page by clicking the **Refresh** link.

What to do next

You can save and export the Orchestrator configuration file so that it can be imported later if needed. See "Export the Orchestrator Configuration," on page 50.

Activate the Service Watchdog Utility

Orchestrator provides a watchdog utility that checks for the activity of the Orchestrator server service. The utility pings the Orchestrator server service periodically, and restarts it if a certain timeout period is exceeded.

By default, the timeout period is set to zero (0), which means that the watchdog utility is deactivated.

You can activate the service watchdog utility by setting the timeout period for the service's response to the ping from the utility. You can set the timeout period for the response from the Orchestrator server service in the `wrapper.conf` configuration file. The `wrapper.conf` file defines the wrapping of the Orchestrator server in the host system.

Prerequisites

The Orchestrator server must be running as a Windows service.

Procedure

1 Navigate to the `wrapper.conf` wrapper configuration file.

   The wrapper configuration file is in the following location:

   `install_directory/app-server/bin/wrapper.conf`

2 Open the `wrapper.conf` file in an editor.

3 Locate the `-wrapper.ping.timeout` parameter in the `wrapper.conf` file, or add it to the file if it does not exist.

4 Set the number of seconds to allow between a ping from the watchdog utility and the response from the service.

   The default timeout is 0 seconds, which means that the utility is deactivated.

   For example, you can increase the timeout period to 30 seconds by setting the parameter as `-wrapper.ping.timeout=30`.

5 Save and close the `wrapper.conf` file.

6 In the Orchestrator configuration interface, select **Startup Options > Restart Service** to restart the Orchestrator server.

You activated the Orchestrator watchdog utility by setting the timeout parameter.

Unwanted Server Restarts

You might experience unwanted server restarts if you have activated the service watchdog utility.

Problem

In certain circumstances, if the response time exceeds the watchdog timeout period, the watchdog utility can falsely detect a JVM error, which causes a server restart.

Cause

The problem occurs when the Orchestrator server is running with a heavy load, for example if you have connected Orchestrator to many vCenter Server instances that are running many virtual machines, or if the server is performing swapping.

Solution

If you experience this behavior, extend the watchdog timeout period by increasing the timeout parameter in the `wrapper.conf` configuration file. If the problem still persists, deactivate the watchdog utility by setting the timeout parameter back to zero (0).

Export the Orchestrator Configuration

Orchestrator Configuration provides a mechanism to export your system settings to a local file. This mechanism allows you to take a snapshot of your system configuration at any moment and import this configuration into a new Orchestrator instance.

VMware recommends that you export and save your configuration settings on a regular basis, especially when making modifications, performing maintenance, or upgrading the system.

Procedure

1   Log in to the Orchestrator configuration interface as `vmware`.

2   On the **General** tab, click **Export Configuration**.

3   (Optional) Enter a password to protect the configuration file.

    Use the same password when you import the configuration.

4   Click **Export**.

5   Click **Save** when prompted.

You can use the `vmo_config_dateReference.vmoconfig` file to clone or to restore the system.

What to do next

For a list of exported configuration settings, see "Orchestrator Configuration Files," on page 50.

Orchestrator Configuration Files

When you export the system configuration, a `vmo_config_dateReference.vmoconfig` file is created locally. It contains all the Orchestrator configuration data.

NOTE   Some of the configuration files that are created during the export are empty. For example, the server configuration data is not exported because the startup options for the Orchestrator server are individual for each machine where the Orchestrator server is installed. These empty files must be reconfigured, even when a working configuration was previously imported.

Table 6-7 contains a list of the settings that are not saved during configuration export.

Table 6-7. Settings Not Saved During Configuration Export

File	Description
certificate	Certificates are not exported. Most certificates are stored in the Orchestrator database. However, the vCenter Server certificate is not stored in the database. You must store it in a separate location, or import it again when you import an Orchestrator configuration.
licenses	Manually imported licenses are not exported. They are stored in the Orchestrator database.
server	The server configuration is reset to Unknown. You must install the Orchestrator server as a Windows service again.

Table 6-8 contains a list of the settings that are saved during configuration export.

Table 6-8. Settings Saved During Configuration Export

File	Description
general	The maximum number of completed events and workflows recorded, and the Web view development and configuration.
network	The IP binding address and the TCP ports used by the different elements of the Orchestrator server.
database	The database configuration.
ldap	The LDAP server configuration.
log	The log settings information.
plug-ins	The list of disabled plug-ins and the account name.
mail plug-in	The SMTP host, SMTP port, user name, password, sender's name, sender's address.
vCenter 4.1 plug-in	The vCenter 4.1 plug-in configuration.
license	The details about the vCenter Server host on which Orchestrator verifies the license key.

Import the Orchestrator Configuration

You can restore the previously exported system configuration if a system failure occurs or when you reinstall Orchestrator.

Procedure

1   Install a new Orchestrator instance on a new server.

2   Log in to the Orchestrator configuration interface as `vmware`.

3   On the **General** tab, click **Import Configuration**.

4   (Optional) Enter the protective password you used when exporting the configuration.

5   Browse to select the `.vmoconfig` file you exported from your previous installation.

6   Click **Import**.

A message states that the configuration is successfully imported. The new system replicates the old configuration completely.

Configure the Maximum Number of Events and Runs

You can define the maximum number of events stored in the database and the maximum number of workflow runs.

Each event corresponds to a change in the state of a workflow or policy and is stored in the database. When the maximum number of events set for a workflow or policy is reached, the database deletes the oldest event to store the new event.

Each time you run a workflow, a workflow token is created in the database. This token contains all parameters related to the running of the workflow. For example, if you run the Test workflow three times, three workflow tokens are created. The three tokens appear in the Orchestrator client above the Test workflow.

Procedure

1   Log in to the Orchestrator configuration interface as `vmware`.

2   On the **General** tab, click **Advanced Configuration**.

3   Fill in the **Max number of events** text box.

    To track every change in your infrastructure, enter `0` (zero=infinite). This means that the server never rolls over, but it might become unavailable. Database administrators must periodically clean the server and archive events.

4   Fill in the **Max number of runs** text box.

    After you reach the maximum number of runs, the rollover process starts. If you do not want the rollover process to start, enter `0` in this text box. If you enter `0`, your database continues to extend.

5   (Optional) To set the default login credentials, fill in the **User name for automatic Web login** and **Password for automatic Web login** text boxes.

    This feature allows you to generate URLs that enable you to run, answer, schedule, or monitor a workflow without having to enter your credentials. Use your default operator credentials for these text boxes.

6   Fill in the **Web view directory** text box.

    This is the root folder from which development Web views are loaded. Files for each Web view must be in a separate subfolder, and the name of this subfolder must be the same as the URL folder defined in the client.

7   (Optional) To put the server in Web view development mode, select the **Enable Web view development** check box.

    In this mode, all elements in the Web view are loaded from the specified Web view directory and not from the Web view content itself.

8   Click **Apply changes**.

Change the Web View SSL Certificate

Orchestrator provides an SSL certificate that controls user access to Web views, such as LCM. You can configure Orchestrator to use a different SSL certificate to control access to Web views. For example, you can change the LCM SSL certificate if your company security policy requires you to use their SSL certificates.

Procedure

1 Create an SSL certificate by running the keytool Java utility at the command prompt.

```
keytool –genkey –alias mySslCertificate –keyalg RSA
```

The keytool utility generates a file called .keystore by using the information and password that you provide when you run the command.

2 Open the C:\Program Files\VMware\Orchestrator\app–server\server\vmo\deploy\jboss–deploy–tomcat \jbossweb–tomcat55.sar\server.xml Orchestrator application server configuration file in an editor.

3 Find the following entry at line 44 in the server.xml file.

```
<!-- Define a SSL HTTP/1.1 Connector on port ${ch.dunes.https-server.port} -->
<Connector address="${jboss.bind.address}" protocol="HTTP/1.1" SSLEnabled="true"
clientAuth="false" emptySessionPath="true"
keystoreFile="${java.home}/lib/security/jssecacerts"
keystorePass="dunesdunes"
maxHttpHeaderSize="8192" maxThreads="100"
port="${ch.dunes.https-server.port}" scheme="https" secure="true"
sslProtocol="TLS" strategy="ms" />
```

4 Change the keystoreFile and keystorePass attributes to refer to the .keystore file and the password you created when you ran the keytool utility.

```
keystoreFile="/PathToKeystore/.keystore"
keystorePass="NewKeystorePassword"
```

5 Save the server.xml file and restart the Orchestrator server.

You changed the SSL certificate that the Orchestrator server uses to control access to Web views.

Define the Server Log Level

In the Orchestrator configuration interface, you can set the level of server log that you require. Changing the log level affects any new messages that the server writes to the server log.

Procedure

1 Log in to the Orchestrator configuration interface as **vmware**.

2 Click **Log**.

3 Select an option from the **Log level** drop-down menu.

Option	Description
FATAL	Only fatal errors are written to the log file.
ERROR	Errors and fatal errors are written to the log file.
WARN	Warnings, errors, and fatal errors are written to the log file.
INFO	Information, warnings, errors, and fatal errors are written to the log file.
DEBUG	Debug information, information messages, warnings, errors, and fatal errors are written to the log file.

Option	Description
ALL	Events are not filtered. All events are written to the log file.
OFF	No entries are written to the log file and no log updates are made.

NOTE   The log displays messages of the selected level and all higher levels. If you select the INFO level, all INFO messages and higher level messages (INFO, WARN, ERROR, and FATAL) are written to the log file.

4   Click **Apply changes**.

5   (Optional) Click the **Generate log report** link to export the log files.

This operation creates a ZIP archive of all logs.

The new log level is applied without server restart to any new messages that the server generates. The logs are stored in *install_directory*\app-server\server\vmo\log\.

Maintenance and Recovery

<div style="text-align: right">7</div>

The **Troubleshooting** tab in the Orchestrator configuration interface allows you to perform several bulk operations related to workflows and tasks. You can use the **Troubleshooting** tab to globally reset the server and remove all traces of previous runs.

Table 7-1 lists the possible bulk operations.

NOTE Before you click a troubleshooting option, make sure the Orchestrator server is stopped.

Table 7-1. Troubleshooting Options

Action	Description
Cancel all running workflows	Marks all running workflows as cancelled in the database, which prevents the server from restarting the workflows on the next reboot. Allows Orchestrator to exit infinite loops.
Delete all workflow runs	Deletes all completed workflow tokens from the Orchestrator database.
Suspend all scheduled tasks	Cancels all scheduled tasks, but does not stop or remove its associated workflow runs.
Clean all server temporary files	Cleans all temporary files that the JBoss server uses to ensure the server persistency. The JBoss server is the application server that underlies the Orchestrator server.
Force plug-in reinstallation when server starts	Used so that a changed plug-in is correctly updated on the next server start.
	NOTE If you change the Orchestrator database after you configure and install the default plug-ins, you must force plug-in reinstallation. Forcing plug-in reinstallation deletes the `install_directory\app-server\server\vmo\plugins \_VSOPluginInstallationVersion.xml` file, which holds the version of the plug-ins already installed and forces plug-in reinstallation. The plug-in is reinstalled with its original content, and any changes are lost.

This chapter includes the following topics:

- "Change the Size of Server Logs," on page 56
- "Maintaining the Orchestrator Database," on page 56
- "Troubleshooting Orchestrator," on page 57

Change the Size of Server Logs

If a server log regenerates multiple times a day, it becomes difficult to determine what causes problems. To prevent this, you can change the default size of the server log. The default size of the server log is 5MB.

Procedure

1 Open the `log4j.xml` file.

   The `log4j.xml` file is in the following location: *installation_directory*\VMware\Orchestrator\app-server \server\vmo\conf

2 Open the `log4j.xml` file in a text editor and locate the following code block:

```
<appender class="org.jboss.logging.appender.RollingFileAppender" name="FILE">
  <errorHandler class="org.jboss.logging.util.OnlyOnceErrorHandler"/>
  <param name="File" value="${jboss.server.home.dir}/log/server.log"/>
  <param name="Append" value="true"/>

  <!-- Rollover at 5MB and allow 4 rollover files -->
  <param name="MaxFileSize" value="5120KB"/>
  <param name="MaxBackupIndex" value="4"/>

  <layout class="org.apache.log4j.PatternLayout">
   <!-- The default pattern: Date Priority [Category] Message\n -->
   <param name="ConversionPattern" value="%d{yyyy-MM-dd HH:mm:ss.SSSZ} %-5p [%c{1}] %m%n"/>
  </layout>
 </appender>
```

3 Change the following lines:

```
<param name="MaxFileSize" value="5120KB"/>
<param name="MaxBackupIndex" value="4"/>
```

   The `MaxFileSize` parameter controls the size of the log file, and the `MaxBackupIndex` parameter controls the number of files for the rollover.

   NOTE Before you save the file, make sure it does not contain typos. If the file contains typos, the logs will be lost.

The system reads this file dynamically. You do not need to reboot the server.

Maintaining the Orchestrator Database

After your Orchestrator database instance and Orchestrator server are installed and operational, perform standard database maintenance processes.

Maintaining your Orchestrator database involves several tasks:

■ Monitoring the growth of the log file and compacting the database log file, as needed. See the documentation for the database type that you are using.

■ Scheduling regular backups of the database.

■ Backing up the database before you upgrade Orchestrator. See your database documentation for information about backing up your database.

Troubleshooting Orchestrator

If you are unable to access the Orchestrator configuration interface or a Web view, such as LCM, you can try restarting the Orchestrator services to troubleshoot the situation.

Restart the Orchestrator Server

You can restart the Orchestrator server if you are unable to access LCM.

Procedure

1   In Windows, select **Start > Programs > Administrative Tools > Services**.

2   Select **VMware vCenter Orchestrator Server**.

3   Right-click and select **Restart**.

Restart the Web Configuration Server

You can restart the Web configuration server if you are unable to access the Orchestrator configuration interface.

Procedure

1   In Windows, select **Start > Programs > Administrative Tools > Services**.

2   Select **VMware vCenter Orchestrator Configuration**.

3   Right-click and select **Restart**.

Controlling Orchestrator Access 8

You can control access to Orchestrator to improve security.

This chapter includes the following topics:

Disable Access to the Orchestrator Client by Nonadministrators

When using LCM, the best practice is to limit access to the Orchestrator client only to administrators.

By default, all users who are granted execute permissions can connect to the Orchestrator client. However, you can limit access to the Orchestrator client to Orchestrator administrators by setting a system property in the `vmo.properties` Orchestrator configuration file.

IMPORTANT   If the `vmo.properties` configuration file does not contain this property, or if the property is set to false, Orchestrator permits access to the Orchestrator client by all users.

Procedure

1   Navigate to the following folder on the Orchestrator server system.

    installation_directory\VMware\Orchestrator\app-server\server\vmo\conf

2   Open the `vmo.properties` configuration file in a text editor.

3   Add the following line to the `vmo.properties` configuration file.

    ```
    #Disable Orchestrator client connection
    com.vmware.o11n.smart-client-disabled = true
    ```

4   Save the `vmo.properties` file.

5   Restart the Orchestrator server.

You disabled access to the Orchestrator client to all users other than members of the Orchestrator administrator LDAP group.

Disable Access to Workflows from Web Service Clients

To prevent malicious attempts from Web service clients to access sensitive servers, you can configure the Orchestrator server to deny access to Web service requests.

By default, Orchestrator permits access to workflows from Web service clients. You disable access to workflows from Web service clients by setting a system property in the Orchestrator configuration file, vmo.properties.

IMPORTANT If the vmo.properties configuration file does not contain this property, or if the property is set to false, Orchestrator permits access to workflows from Web services.

Procedure

1 Navigate to the following folder on the Orchestrator server system.

    installation_directory\VMware\Orchestrator\app-server\server\vmo\conf

2 Open the vmo.properties configuration file in a text editor.

3 Add the following line to the vmo.properties configuration file.

    ```
    #Disable Web service access
    com.vmware.o11n.web-service-disabled = true
    ```

4 Save the vmo.properties file.

5 Restart the Orchestrator server.

You disabled access to workflows Web service clients. The Orchestrator server only answers Web service client calls from the echo() or echoWorkflow() methods, for testing purposes.

Installing and Configuring LCM

Installing LCM 9

After you have installed vCenter Orchestrator, you can install vCenter Lifecycle Manager.

This chapter includes the following topics:

Installation Prerequisites

Make sure that your system meets the installation prerequisites before you install LCM on Microsoft Windows.

Table 9-1. Installation Prerequisites

Component	Description
VMware vCenter Orchestrator 4.1	
VMware vSphere™	Requirements: ■ vCenter Server 4.1 or vCenter Server 4.0 Update 2 ■ The Sysprep utility for the guest OS must be available in the proper directory on the vCenter Server.
VMware ESX™	Support for ESX depends on the version of vCenter Server that you are using. See the documentation for the relevant version of vCenter Server.
ActiveDirectory domain	
Sample ActiveDirectory groups that correspond to LCM roles	The roles are: ■ LCM Administrator ■ LCM IT Staff ■ LCM Approver ■ LCM Tech Requester ■ LCM Requester
Appropriate permissions for the LCM groups	Include the following permissions: ■ Allow the Orchestrator Administrator to deploy from vCenter Server templates. ■ RDP access in the guest operating system. Use xrdp for Linux virtual machines.

Table 9-1. Installation Prerequisites (Continued)

Component	Description
LCM database	Choose one of the following approaches: ■ Use the same database as Orchestrator. ■ Use a separate database for LCM (recommended). NOTE Because of CPU and memory usage, you should consider hosting the LCM database and the Orchestrator server on different machines on a local network with low latency.
Static account for each vCenter Server that LCM and Orchestrator can use	
DHCP server and fixed range of IP addresses for new virtual machines	

Required vCenter Server Privileges

To manage virtual machines, an LCM user must have a minimum set of privileges in vCenter Server.

The following privileges are required.

■ **Datastore>Allocate Space**

■ **Datastore>Browse Datastore**

■ **Folder>Create Folder**

■ **Host Profile>View**

■ **Resource>Assign virtual machine to resource pool**

■ **Resource>Create resource pool**

■ **Virtual Machine>Configuration>Change CPU count**

■ **Virtual Machine>Configuration>Change resource**

■ **Virtual Machine>Configuration>Memory**

■ **Virtual Machine>Configuration>Modify device Settings**

■ **Virtual Machine>Interaction>Console interaction**

■ **Virtual Machine>Interaction>Power Off**

■ **Virtual Machine>Interaction>Power On**

■ **Virtual Machine>Interaction>Reset**

■ **Virtual Machine>Interaction>Suspend**

■ **Virtual Machine>Inventory>Create from existing**

■ **Virtual Machine>Inventory>Remove**

■ **Virtual Machine>Inventory>Unregister**

■ **Virtual Machine>Provisioning>Clone template**

■ **Virtual Machine>Provisioning>Clone virtual machine**

■ **Virtual Machine>Provisioning>Customize**

■ **Virtual Machine>Provisioning>Deploy template**

■ **Virtual Machine>State>Create Snapshot**

■ **Virtual Machine>State>Revert to snapshot**

Install Lifecycle Manager

You must install LCM through the Orchestrator configuration interface.

Procedure

1   Log in to the Orchestrator configuration interface.

    http://*orchestrator_server*:8282

2   On the **General** tab, click **Install Application**.

3   Browse to select the LCM `.vmoapp` file.

> ⚠️ **CAUTION**   If you are running Orchestrator on Windows Server 2008, you must manually rename the file extension to `.vmoapp`. When you download the `.vmoapp` file, Windows Server 2008 automatically renames the file extension to `.zip`, which is not supported by the Orchestrator configuration interface.

4   Click **Install**.

5   On the **Licences** tab, click **Plug-in Licences**.

6   Type the LCM serial number and click **Apply changes**.

Configuring LCM Database Options

You must configure the options for the LCM database table and the networking database table in the Orchestrator configuration interface.

■ Configure the LCM Database Plug-In on page 65

The LCM database table contains virtual-machine-specific data that is managed by LCM, such as when the virtual machine was created, who created it, and other specifications.

■ Configure the Networking Database Plug-In on page 66

The networking database table contains data related to the management of the IP addresses.

Configure the LCM Database Plug-In

The LCM database table contains virtual-machine-specific data that is managed by LCM, such as when the virtual machine was created, who created it, and other specifications.

Procedure

1   Log in to the Orchestrator configuration interface.

    http://*orchestrator_server*:8282

2   On the **vCenter Lifecycle Manager** tab, select the database connection type.

Option	Description
Same as vCO	Select this option to store LCM data in the Orchestrator database.
Custom	Select this option to store LCM data in a database different from the Orchestrator database.
	NOTE The best practice is to use a separate database for LCM.
	Depending on the type of database you are connecting to, the required information might vary. For a list of the connection parameters that you might be required to specify, see "Database Connection Parameters," on page 40.

3   Click **Apply changes**.

Configure the Networking Database Plug-In

The networking database table contains data related to the management of the IP addresses.

Procedure

1   Log in to the Orchestrator configuration interface.

    http://*orchestrator_server*:8282

2   On the **Networking** tab, select the database connection type.

Option	Description
Same as vCO	Select this option to store LCM networking data in the Orchestrator database.
Custom	Select this option to store LCM networking data in a database different from the Orchestrator database.
	NOTE The best practice is to use a separate database for LCM.
	Depending on the type of database you are connecting to, the required information might vary. For a list of the connection parameters that you might be required to specify, see "Database Connection Parameters," on page 40.

3   Click **Apply changes**.

What to do next

On the **Startup Options** tab, click **Restart service** to apply the plug-ins configuration.

Configuring LCM

<div style="text-align: right; font-size: large;">**10**</div>

You must configure LCM before you can use it. The configuration process involves setting up the virtual machine naming convention, specifying groups, and selecting date and currency formats. You can also configure role-based attributes.

This chapter includes the following topics:

Check Configuration Readiness

Before you start configuring LCM, you can check whether the configuration service is ready.

Procedure

1 Log in to the Orchestrator configuration interface.

http://*orchestrator_server*:8282

2 Verify that all status indicators display a green circle.

3 On the **General** tab, check the server status.

4 If the status is not Running, click the **Startup Options** tab and click **Start service**.

Initial Configuration of Lifecycle Manager

You must complete the initial configuration of LCM when you run LCM for the first time.

Procedure

1   Go to `http://orchestrator_server:8280/vmo/lifecycle` to log in to LCM for the first time.

    You need to log in with the credentials of a user who is a member of the administrator group that is selected in Orchestrator.

2   (Optional) Edit the default virtual machine naming convention.

    The default is lcm-0001, lcm-0002, and so on.

3   Choose whether to allow approvers and IT staff to manually overwrite the default name.

4   Select a currency from the drop-down menu.

5   Select the date format that you want to use.

6   Accept the default setting for advanced options and click **Next**.

    You can edit the advanced options later.

7   Specify which groups belong to the different roles and click **Next** when you are done.

    You can type the first few letters of the group name and let the LDAP search match the choices, or you can click **Search** to browse the LDAP inventory.

8   Accept the approvals, archiving, and notification defaults, and click **Submit**.

    You can change these values later. The LCM Web view is started.

> ⚠️ **CAUTION** Do not change the LDAP settings in Orchestrator after submitting the configuration. This might result in a serious error that requires using a backup for recovery.

9   Log in to LCM again as the LCM Administrator.

    The LCM Administrator must be a member of the LCM Administrators group that you just configured.

Configure the LCM Web View

The Web UI of an application is called a Web view. For example, the front end of LCM is a Web view. You can configure custom settings for the LCM Web view.

Procedure

1   Log in to LCM as an administrator.

2   Click the **Configuration** view.

3   In the left pane, click **Edit Advanced Configuration**.

4   Under **Display**, choose whether you want LCM to display the details of an execution token after submitting a workflow.

    You can also limit the number of elements displayed on a single page.

5   In the **Webview URL** text box, you can type a custom URL for the LCM Web view.

6   Click **Submit**.

Set Approval Requirements

Virtual machines are decommissioned on the date selected by the requester when requesting the machine. LCM notifies the owner of the virtual machine five days before the decommissioning date with the option to request an extension. You can specify whether approval is required when virtual machines are requested, extended, or modified.

Procedure

1   Log in to LCM as an administrator.

2   Click the **Configuration** view.

3   Click **Edit Approval Modes**.

4   Under **Creation**, **Extension**, and **Customization changes**, select whether approval is required.

     You can change these values later.

5   Click **Submit**.

If you enable the two approvals under **Customization changes**, an LCM Approver and an LCM IT Staff user must approve each request for customization changes.

Configure Archiving Settings

Virtual machines can be archived instead of deleted when they are decommissioned.

Procedure

1   Log in to LCM as an administrator.

2   Click the **Configuration** view.

3   Click **Edit Archiving**.

4   Under **Archive configuration**, choose whether to archive by default.

5   If you selected **Yes**, in **Destination Datastores**, select a datastore or an array of datastores to store the archive.

     The datastore must be accessible from the ESX host running the virtual machine to be archived. The archive is placed in the first available datastore from the array. If no datastore has sufficient space, the archive process fails.

6   Click **Submit**.

Change Authorization Groups

You can modify the types of changes that each role can make.

For information about role-to-task mapping, see "User Roles and Permitted Tasks," on page 14.

> ⚠ **CAUTION**   Changing authorization groups can be a risk for existing users. Existing users might be unable to access their virtual machine requests as a result of such changes.

Procedure

1   Log in to LCM as an administrator.

2   Click the **Configuration** view.

3   Click **Edit Authorization Groups**.

4   Under **Management Groups**, select or type appropriate values for the groups.

5   Under **Requester Groups**, select or type appropriate values for the groups.

6   Click **Submit**.

Change the Naming Convention for Virtual Machines

You can change the naming convention for a virtual machine. The default is **lcm-####**.

Procedure

1   Log in to LCM as an administrator.

2   Click the **Configuration** view.

3   Click **Edit Base Name**.

4   Under **Default Base Name Convention**, in the **Name** text box, type the naming convention.

5   Choose whether to allow an LCM Approver or an LCM IT Staff user to change the virtual machine name when approving a request.

6   Click **Submit**.

Enable Email Notifications

LCM users can be sent emails when they are required to perform an action. For example, an LCM Approver can receive an email when required to approve or reject a virtual machine request. You can enable email notifications.

Procedure

1   Log in to LCM as an administrator.

2   Click the **Configuration** view.

   If the **Mail** icon ( ) does not appear next to the **Configuration** icon ( ), email notifications are disabled.

3   To enable email notifications, click **Edit Email Notifications** in the left pane.

4   Under **Activation**, click **Yes**.

5   Type the email addresses for the LCM Administrator, LCM IT Staff, and LCM Approver roles.

6   Click **Submit**.

You can configure email notification content the next time you log in to LCM as an administrator.

Configure Email Notification Content

If you have email options configured in Orchestrator, you can configure the content of LCM email notifications.

For information about setting up email options in Orchestrator, see "Define the Default SMTP Connection," on page 45.

Procedure

1   Log in to LCM as an administrator.

2   Click the **Configuration** view.

3   Click the **Mail** icon ( ).

   A list of actions for which you can set up notifications appears. You can also activate or deactivate all notifications.

4   Click a notification ( ) in the left pane.

    The details about the notification appear in the right pane.

5   Click **Edit**.

6   For each notification, specify whether to enable it, who the recipients are, what appears in the Subject field, and a default email body text.

    You can use the following variables in the email body:

    ■   *#vmName* – Virtual machine name

    ■   *#decommissionDate* – Date that the virtual machine request is set to be decommissioned

    ■   *#error* – Error message

    ■   *#requester* – Name of the requester

    ■   *#ipAddress* – IP address of the virtual machine, if the request is available and the virtual machine is powered on

    ■   *#webviewUrl* – URL of the LCM Web view

    These variables are changed to their corresponding values when the email is generated.

7   Click **Submit**.

8   Repeat these steps for each email notification that you want to create.

Configure Currency and Date Formats

You can configure the currency and date formats.The price of a virtual machine is estimated in the currency that you select.

Procedure

1   Log in to LCM as an administrator.

2   Click the **Configuration** view.

3   Click **Edit Format (Currency, Date)**.

4   Select a currency format.

5   Select a date format.

6   Click **Submit**.

Upgrading Orchestrator and LCM

Upgrading to Orchestrator 4.1 and LCM 1.2

11

If you are using LCM 1.1.x and Orchestrator 4.0.1, you can upgrade to LCM 1.2 and Orchestrator 4.1.

You must upgrade both LCM and Orchestrator. LCM 1.1.x is not compatible with Orchestrator 4.1, and LCM 1.2 is not compatible with Orchestrator 4.0.1.

This chapter includes the following topics:

Backing Up Database Tables

Before upgrading, you should back up your LCM database table, LCM networking database table, and Orchestrator database table.

The LCM database table contains virtual-machine-specific data that is managed by LCM, such as when the virtual machine was created, who created it, and other specifications.

The LCM networking database table contains data related to the management of the IP addresses.

The Orchestrator database table contains all data related to Orchestrator. If you are using a common database for LCM and Orchestrator, it also contains all data related to LCM.

NOTE Backing up database tables is optional, but you should consider using backup for databases in a production environment. The backup procedure depends on your database vendor.

Back Up Modified and Custom Orchestrator Elements

When you upgrade Orchestrator, elements with a higher version number silently overwrite the elements stored in the Orchestrator database. For example, if you have edited any standard workflows, actions, policies, Web views, or configuration elements and you import a package containing the same elements with higher version number, your changes to the elements are lost. To make modified and custom elements available after the upgrade, you must export them in a package before you start the upgrade procedure.

Prerequisites

See the *vCenter Orchestrator Administration Guide* for details about creating and exporting packages.

Log in to the Orchestrator client application.

Procedure

1   Create a package that contains all the Orchestrator elements that you created or edited.

2   Export the package.

The upgrade procedure cannot affect the Orchestrator elements that you modified or created.

What to do next

Upgrade Orchestrator and restore the configuration data. In the Orchestrator client application, import the package that contains your custom elements and confirm the import of elements with lower version numbers. For details about importing a package, see *vCenter Orchestrator Administration Guide*.

Upgrading an Installation Running on a 32-Bit Machine

If Orchestrator 4.0.1 and LCM 1.1.x are installed on a 32-bit machine, you must install Orchestrator 4.1 and LCM 1.2 on a new 64-bit machine. You should use the same IP address and host name for the 64-bit machine that you used for the source 32-bit machine.

To upgrade to Orchestrator 4.1 and LCM 1.2, you must export the Orchestrator configuration settings, stop the Orchestrator server, install Orchestrator 4.1 and LCM 1.2 on a 64-bit machine, import the configuration settings, upgrade the infrastructure, configure the vCenter Server plug-in, and start the Orchestrator server.

IMPORTANT   Because LCM 1.1.x uses the VMware Infrastructure 3.5 plug-in and LCM 1.2 uses the vCenter Server 4.1 plug-in, your environment's configuration is not migrated automatically. You must manually copy the configuration of the VMware Infrastructure 3.5 plug-in and replicate it when you configure the vCenter Server 4.1 plug-in.

To complete the upgrade, you must perform these procedures:

1   "Export the Orchestrator Configuration," on page 50

2   "Stop the Orchestrator Server," on page 76

3   Chapter 5, "Install Orchestrator," on page 25

4   "Install Lifecycle Manager," on page 65

5   "Import the Orchestrator Configuration," on page 51

6   "Upgrading the vCenter Server Environment," on page 77

7   "Configure the vCenter Server 4.1 Plug-In," on page 46

8   "Start the Orchestrator Server," on page 48

⚠ **CAUTION**   You must perform the procedures in this exact order. If you start the Orchestrator server before you complete the other procedures, your infrastructure elements might become unlinked. For instructions about relinking unlinked elements, see the *vCenter Lifecycle Manager Administration Guide*.

Stop the Orchestrator Server

Before you start upgrading to Orchestrator 4.1 and LCM 1.2, you must stop the Orchestrator server on the 32-bit Orchestrator 4.0.1 machine.

Procedure

1   In Windows, select **Start > Programs > Administrative Tools > Services**.

2   Select **VMware vCenter Orchestrator Server**.

3   Right-click **VMware vCenter Orchestrator Server** and select **Stop**.

Upgrading an Installation Running on a 64-Bit Machine

If Orchestrator 4.0.1 and LCM 1.1.x are installed on a 64-bit machine, you can install Orchestrator 4.1 and LCM 1.2 on the same machine.

To upgrade to Orchestrator 4.1 and LCM 1.2, you must export the Orchestrator configuration settings, uninstall the existing installation, install Orchestrator 4.1 and LCM 1.2, import the configuration settings, upgrade the infrastructure, configure the vCenter Server plug-in, and start the Orchestrator server.

IMPORTANT   Because LCM 1.1.x uses the VMware Infrastructure 3.5 plug-in and LCM 1.2 uses the vCenter Server 4.1 plug-in, your environment's configuration is not migrated automatically. You must manually copy the configuration of the VMware Infrastructure 3.5 plug-in and replicate it when you configure the vCenter Server 4.1 plug-in.

To complete the upgrade, you must perform these procedures:

1   "Export the Orchestrator Configuration," on page 50

2   Chapter 12, "Uninstall LCM and Orchestrator," on page 79

3   Chapter 5, "Install Orchestrator," on page 25

4   "Install Lifecycle Manager," on page 65

5   "Import the Orchestrator Configuration," on page 51

6   "Upgrading the vCenter Server Environment," on page 77

7   "Configure the vCenter Server 4.1 Plug-In," on page 46

8   "Start the Orchestrator Server," on page 48

⚠ CAUTION   You must perform the procedures in this exact order. If you start the Orchestrator server before you complete the other procedures, your infrastructure elements might become unlinked. For instructions about relinking unlinked elements, see the *vCenter Lifecycle Manager Administration Guide*.

Upgrading the vCenter Server Environment

If you are using a VirtualCenter 2.5 environment or a version of vCenter Server earlier than 4.0 Update 2, you must upgrade to vCenter Server 4.1 or vCenter Server 4.0 Update 2. If you are using vCenter Server 4.0 Update 2, the upgrade to vCenter Server 4.1 is optional.

For detailed upgrade instructions, see the *vSphere Upgrade Guide*.

Uninstall LCM and Orchestrator 12

You can remove LCM from your system by uninstalling Orchestrator. You can remove the Orchestrator client and server components from your system by using the Windows Add or Remove Programs utility from the Control Panel.

Prerequisites

Save the Orchestrator system settings to a local file. For details, see "Export the Orchestrator Configuration," on page 50.

Procedure

1   From the Windows Start menu, select **Settings > Control Panel > Add or Remove Programs**.

2   Select vCenter Orchestrator and click **Remove**.

3   Click **Uninstall** in the Uninstall vCenter Orchestrator dialog.

    A message confirming that all items were successfully removed appears.

4   Click **Done** to close the uninstaller.

Orchestrator and LCM are uninstalled from your system.

Index