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.
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
## Contents

Updated Information 5

About This Book 7

1 Introduction to VMware vCenter Orchestrator 9
   Key Features of the Orchestrator Platform 9
   Orchestrator User Roles and Related Tasks 10
   Orchestrator Architecture 11
   Deprecated Features in Orchestrator 4.1 12

2 Orchestrator System Requirements 13
   Hardware Requirements for Orchestrator 13
   Operating Systems Supported by Orchestrator 13
   Supported Directory Services 13
   Browsers Supported by Orchestrator 14
   Orchestrator Database Requirements 14
   Level of Internationalization (i18n) Support 14

3 Orchestrator Components Setup Guidelines 17
   Orchestrator Configuration Maximums 17
   vCenter Server Setup 17
   Directory Services Setup 18
   Orchestrator Database Setup 18

4 Installing and Upgrading Orchestrator 19
   Install vCenter Server and Orchestrator 19
   Install Orchestrator Standalone 21
   Install the Orchestrator Client on a 32-Bit Machine 23

5 Upgrading to Orchestrator 4.1 and Migrating the Orchestrator Data 25
   Upgrading an Orchestrator Instance Running on a 32-Bit Machine 25
   Back Up the Orchestrator Configuration Data 26
   Back Up Modified and Custom Orchestrator Elements 27
   Install Orchestrator with vCenter Server on a 64-Bit Machine and Import the Configuration Data 27
   Upgrading an Orchestrator Instance Running on a 64-Bit Machine 29

6 Uninstall Orchestrator 31

7 Configuring Orchestrator 33
   Start the Orchestrator Configuration Service 34
**Updated Information**

The vCenter Orchestrator Installation and Configuration Guide is updated with each release of the product or when necessary.

This table provides the update history of the vCenter Orchestrator Installation and Configuration Guide.

<table>
<thead>
<tr>
<th>Revision</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>EN-000321-03</td>
<td>- Removed the information related to the experimental support of OpenLDAP, PostgreSQL and MySQL.</td>
</tr>
<tr>
<td></td>
<td>- Updated the instructions in “Generate the LDAP Connection URL,” on page 40.</td>
</tr>
<tr>
<td></td>
<td>- Updated the instructions in “Specify the Browsing Credentials,” on page 42.</td>
</tr>
<tr>
<td></td>
<td>- Updated the instructions in “Define the LDAP User and Group Lookup Paths,” on page 42.</td>
</tr>
<tr>
<td></td>
<td>- Updated Step 5 in “Configure the Database Connection,” on page 45.</td>
</tr>
<tr>
<td></td>
<td>- Updated the instructions in “Configure SQL Server Express to Use with Orchestrator,” on page 47.</td>
</tr>
<tr>
<td></td>
<td>- Updated Step 4 in “Import the Plug-In Licenses,” on page 60.</td>
</tr>
<tr>
<td></td>
<td>- Minor revisions</td>
</tr>
<tr>
<td></td>
<td>- Updated Step 1 in “Log In to the Orchestrator Configuration Interface,” on page 34.</td>
</tr>
<tr>
<td></td>
<td>- Updated prerequisites and note in “Configure the Database Connection,” on page 45.</td>
</tr>
<tr>
<td></td>
<td>- Updated the instructions in “Configure the Maximum Number of Events and Runs,” on page 59.</td>
</tr>
<tr>
<td></td>
<td>- Added instructions about using Microsoft SQL Express with Orchestrator in “Configure SQL Server Express to Use with Orchestrator,” on page 47.</td>
</tr>
<tr>
<td></td>
<td>- Added information about log level ALL in “Define the Server Log Level,” on page 61.</td>
</tr>
<tr>
<td></td>
<td>- Removed cross-references before tables and figures.</td>
</tr>
<tr>
<td>EN-000321-00</td>
<td>Initial release of Orchestrator 4.1.</td>
</tr>
</tbody>
</table>
About This Book

The *VMware vCenter Orchestrator Installation and Configuration Guide* provides information and instructions about installing, upgrading and configuring VMware® vCenter Orchestrator.

Intended Audience

This book is intended for advanced vCenter administrators and experienced system administrators who are familiar with virtual machine technology and datacenter operations.

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.
VMware vCenter Orchestrator is a development and process-automation platform that provides a library of extensible workflows to allow you to create and run automated, configurable processes to manage the VMware vCenter infrastructure as well as other VMware and third-party technologies.

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

This chapter includes the following topics:

- “Key Features of the Orchestrator Platform,” on page 9
- “Orchestrator User Roles and Related Tasks,” on page 10
- “Orchestrator Architecture,” on page 11
- “Deprecated Features in Orchestrator 4.1,” on page 12

### Key Features of the Orchestrator Platform

Orchestrator is composed of three distinct layers: an orchestration platform that provides the common features required for an orchestration tool, a plug-in architecture to integrate control of subsystems, and a library of workflows. Orchestrator is an open platform that can be extended with new plug-ins and libraries, and can be integrated into larger architectures through a SOAP API.

The following list presents the key Orchestrator features.

- **Persistence**
  Production grade external databases are used to store relevant information, such as processes, workflow states, and configuration information.

- **Central management**
  Orchestrator provides a central way to manage your processes. The application server-based platform, with full version history, allows you to have scripts and process-related primitives in one place. This way, you can avoid scripts without versioning and proper change control spread on your servers.

- **Check-pointing**
  Every step of a workflow is saved in the database, which allows you to restart the server without losing state and context. This feature is especially useful for long-running processes.

- **Versioning**
  All Orchestrator Platform objects have an associated version history. This feature allows basic change management when distributing processes to different project stages or locations.
Scripting engine
The Mozilla Rhino JavaScript engine provides a way to create new building blocks for Orchestrator Platform. The scripting engine is enhanced with basic version control, variable type checking, name space management and exception handling. It can be used in the following building blocks:
- Actions
- Workflows
- Policies

Workflow engine
The workflow engine allows you to capture business processes. It uses the following objects to create a step-by-step process automation in workflows:
- Workflows and actions that Orchestrator provides.
- Custom building blocks created by the customer
- Objects that plug-ins add to Orchestrator

Policy engine
The policy engine allows monitoring and event generation to react to changing conditions in the Orchestrator server or plugged-in technology. Policies can aggregate events from the platform or any of the plug-ins, which allows you to handle changing conditions on any of the integrated technologies.

Web 2.0 front end
The Web 2.0 front end allows you to integrate Orchestrator functions into Web-based interfaces, using Web views. For example, you can create Web views that add buttons to start workflows from a page in your company’s Intranet. It provides a library of user customizable components to access vCO orchestrated objects and uses Ajax technology to dynamically update content without reloading complete pages.

Security
Orchestrator provides the following advanced security functions:
- Public Key Infrastructure (PKI) to sign and encrypt content imported and exported between servers
- Digital Rights Management (DRM) to control how exported content might be viewed, edited and redistributed
- Secure Sockets Layer (SSL) encrypted communications between the desktop client and the server and HTTPS access to the Web front end.
- Advanced access rights management to provide control over access to processes and the objects manipulated by these processes.

Orchestrator User Roles and Related Tasks
vCenter Orchestrator provides different tools and interfaces based on the specific responsibilities of the two global user roles: Administrators and End Users.

Administrators
This role has full access to all of the Orchestrator platform capabilities. Basic administrative tasks include the following items:
- Installing and configuring Orchestrator
- Managing access rights for Orchestrator and applications
- Importing and exporting packages
- Enabling and disabling Web views
Running workflows and scheduling tasks
Managing version control of imported elements
Creating new workflows and plug-ins

Developers
This role has full access to all of the Orchestrator platform capabilities. Developers are granted access to the Orchestrator client interface and have the following responsibilities:
- Creating applications to extend the Orchestrator platform functionality
- Automating processes by customizing existing workflows and creating new workflows and plug-ins
- Customizing Web front ends for these processes, using Web 2.0

End Users
Users in this role are granted access to only the Web front end. They can run and schedule workflows and policies that you make available in a browser by using Web views.

Orchestrator Architecture
Orchestrator contains a workflow library and workflow engine to allow you to create and run workflows that automate orchestration processes. You run workflows on the objects of different technologies that Orchestrator accesses through a series of plug-ins.

Orchestrator provides a standard set of plug-ins, including a plug-in to VMware vCenter Server, to allow you to orchestrate tasks in the different environments that the plug-ins expose.

Orchestrator also presents an open architecture to allow you to plug in external third-party applications to the orchestration platform. You can run workflows on the objects of the plugged-in technologies that you define yourself. Orchestrator connects to a directory services server to manage user accounts, and to a database to store information from the workflows that it runs. You can access Orchestrator and the workflows and objects it exposes through the Orchestrator client interface, through a Web browser, or through Web services.

Figure 1-1 shows the architecture of Orchestrator.

Figure 1-1. VMware vCenter Orchestrator Architecture

NOTE The VMware Infrastructure 3 and Microsoft plug-ins are not installed by default.
Deprecated Features in Orchestrator 4.1

The following features are deprecated as of Orchestrator 4.1. Development of these features is not supported in releases of Orchestrator later than 4.1.

- Authorizations
- OGNL expressions in workflow presentations
- Policies
Orchestrator System Requirements

Your system must meet the technical requirements that are necessary to install and configure VMware vCenter Orchestrator.

This chapter includes the following topics:

- “Hardware Requirements for Orchestrator,” on page 13
- “Operating Systems Supported by Orchestrator,” on page 13
- “Supported Directory Services,” on page 13
- “Browsers Supported by Orchestrator,” on page 14
- “Orchestrator Database Requirements,” on page 14
- “Level of Internationalization (i18n) Support,” on page 14

Hardware Requirements for Orchestrator

Verify that 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

For a list of the operating systems supported by Orchestrator, see the VMware vSphere Compatibility Matrixes guide.

Supported Directory Services

Orchestrator requires a working LDAP server on your infrastructure.

Orchestrator supports these directory service types.

- Windows Server 2003 Active Directory
- Windows Server 2008 Active Directory
- Novell eDirectory Server 8.8.3
- Sun Java Directory Server Version 6.3
Browsers Supported by Orchestrator

The Orchestrator configuration and Web view interfaces require a Web browser.

You must have one of the following browsers to connect to the Orchestrator configuration interface and Web views.

- Microsoft Internet Explorer 7.0
- Mozilla Firefox 3.0 (build 3.0.6 or later)
- Mozilla Firefox 3.5

Orchestrator Database Requirements

Orchestrator requires you to have a database that is separate from the standard vCenter database. For small deployments and proof-of-concept purposes, you can use the SQL Server Express database that is bundled with vCenter Server.

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

For a list of the databases supported by Orchestrator, see the VMware vSphere Compatibility Matrixes guide.

Level of Internationalization (i18n) Support

Orchestrator is compliant with i18n level 1. Although Orchestrator is not localized, it can run on a non-English operating system and handle non-English text.

Non-ASCII Character Support in Orchestrator

*Table 2-1* displays the level of internationalization compliance and limitations in Orchestrator GUI data entries.

<table>
<thead>
<tr>
<th>Item</th>
<th>Support for Non-ASCII Characters</th>
<th>Description Field</th>
<th>Name Field</th>
<th>Input and Output Parameters</th>
<th>Attributes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Action</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Folder</td>
<td>Yes</td>
<td>Yes</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Configuration element</td>
<td>Yes</td>
<td>Yes</td>
<td>-</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Package</td>
<td>Yes</td>
<td>Yes</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Policy</td>
<td>Yes</td>
<td>Yes</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Policy template</td>
<td>Yes</td>
<td>Yes</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Resource element</td>
<td>Yes</td>
<td>Yes</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Web view</td>
<td>Yes</td>
<td>Yes</td>
<td>-</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Workflow</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Workflow presentation display group and input step</td>
<td>Yes</td>
<td>Yes</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>
Non-ASCII Character Support for Oracle Databases

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.
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:
- “Orchestrator Configuration Maximums,” on page 17
- “vCenter Server Setup,” on page 17
- “Directory Services Setup,” on page 18
- “Orchestrator Database Setup,” on page 18

**Orchestrator Configuration Maximums**

When you configure Orchestrator, verify that you stay at or below the supported maximums.

<table>
<thead>
<tr>
<th>Item</th>
<th>Maximum</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connected vCenter Server systems</td>
<td>10</td>
</tr>
<tr>
<td>Connected ESX/ESXi servers</td>
<td>300</td>
</tr>
<tr>
<td>Connected virtual machines spread over vCenter Server systems</td>
<td>15000</td>
</tr>
<tr>
<td>Concurrent running workflows</td>
<td>300</td>
</tr>
</tbody>
</table>

**vCenter Server Setup**

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

For a list of the supported versions of vCenter Server, see *VMware Product Interoperability Matrix*.

**Note** You can run multiple vCenter Server 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 Server, a 100Mb line is mandatory.
Directory Services Setup

Orchestrator requires a connection to an LDAP 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. Limit the users to targeted groups that need access, rather than to whole organizations with many users who do not need access. Depending on the combination of database and directory service you choose, the resources you need can vary. For recommendations, see the documentation for your LDAP server.

Orchestrator Database Setup

Orchestrator requires a database to store workflows and actions.

Orchestrator server supports Oracle and Microsoft SQL Server databases. Orchestrator can work with Microsoft SQL Server Express in small-scale environments consisting of up to 5 hosts and 50 virtual machines.

For details about using SQL Server Express with Orchestrator, see “Configure SQL Server Express to Use with Orchestrator,” on page 47.

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

Storing your database plug-ins in a database separate from the one that Orchestrator uses results in 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 50KB per vCenter Server object and 4KB per workflow run.

**CAUTION** Verify that at least 1GB of free disk space is available on the machine where the Orchestrator database is installed and on the machine where the Orchestrator server is installed.

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

Orchestrator consists of a server component and a client component. You can install the Orchestrator components on the machine where vCenter Server is installed or on a separate machine. To improve performance, install the Orchestrator server component on a separate machine.

You can install the Orchestrator configuration server on 64-bit Windows machines only. The Orchestrator client can run on both 32-bit and 64-bit Windows machines.

To install Orchestrator, you must be either a local Administrator or a domain user that is a member of the Administrators group.

This chapter includes the following topics:

- “Install vCenter Server and Orchestrator,” on page 19
- “Install Orchestrator Standalone,” on page 21
- “Install the Orchestrator Client on a 32-Bit Machine,” on page 23

Install vCenter Server and Orchestrator

When you install VMware vCenter Server, Orchestrator is silently installed on your system as an additional component.

You can install vCenter Server 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 the installation package is not supported by the processor type.

**Note** To install the vCenter Server on a drive other than C:, verify that the C:\WINDOWS\Installer folder is large enough to install the Microsoft Windows Installer .msi file. If the folder is not large enough, your vCenter Server installation might fail.

For a list of required ports, see the *ESX and vCenter Server Installation Guide*.

**Prerequisites**

See vCenter Server installation prerequisites in the *ESX and vCenter Server Installation Guide*. 
Procedure

1. Download the vCenter Server installation package from the VMware Web site.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use ISO image</td>
<td>The filename is VMware-VIMSetup-xx-4.a.b-yyyy.iso, where a and b are major and minor version, xx is the two-character language code, and yyyy is the build number.</td>
</tr>
<tr>
<td>Use ZIP archive</td>
<td>The filename is VMware-VIMSetup-xx-4.a.b-yyyy.zip, where a and b are major and minor version, xx is the two-character language code, and yyyy is the build number.</td>
</tr>
</tbody>
</table>

2. Extract the files from the archive and in the C:\install_directory\ directory, double-click the autorun.exe file.

3. When the vCenter Server Installer appears, click vCenter Server.

4. Select a language for the installer and click OK.

5. When the Welcome page appears, click Next.

6. Select I agree to the terms in the license agreement and click Next.

7. Type your user name, organization, and vCenter Server license key, and click Next.

8. Select the type of database to use.

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>To use the bundled database</td>
<td>Click Install SQL Server 2005 Express instance (for small-scale deployments). This database is suitable for deployments of up to 5 hosts and 50 virtual machines.</td>
</tr>
<tr>
<td>To use an existing database</td>
<td>Click Use an existing supported database and select your database from the list. Type the user name and password for the DSN and click Next. If your database is a local SQL Server database using Windows NT authentication, leave the user name and password fields blank. If you specify a remote SQL Server database that uses Windows NT authentication, the database user and the logged-in user on the vCenter Server machine must be the same.</td>
</tr>
</tbody>
</table>

A dialog box might appear, warning you that the DSN points to an older version of a repository that must be upgraded. If you click Yes, the installer upgrades the database schema, making the database irreversibly incompatible with previous vCenter versions.

9. Specify the account for the vCenter Service to run in.

   - Click Next to use the SYSTEM account. You cannot use the SYSTEM account if you are using Windows authentication for SQL Server.

   - Deselect Use SYSTEM Account, accept the default Administrator account name and password, and click Next.

   - Deselect Use SYSTEM Account and enter a different Administrator account name and password.

10. Either accept the default destination folders or click Change to select another location, and click Next.

    The installation path cannot have commas (,) or periods (.)
11 Select the installation mode and click Next.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create a standalone VMware vCenter Server instance</td>
<td>Use this option for standalone mode or for the first vCenter Server installation when you are forming a new linked mode group.</td>
</tr>
<tr>
<td>Join a VMware vCenter Server group using linked mode to share information</td>
<td>Enables the vSphere client to view, search, and manage data across multiple vCenter Server systems. Use this option for the second and subsequent vCenter Server installations when you are forming a linked mode group.</td>
</tr>
</tbody>
</table>

12 (Optional) If you join a group, enter the fully qualified domain name and LDAP port number of any remote vCenter Server system and click Next.

In some cases, you can enter the IP address instead of the fully qualified domain name. To help ensure connectivity, the best practice is to use the fully qualified domain name. For IPv6, unless both the local and the remote machine are in IPv6 mode, you must enter the fully qualified domain name of the remote machine instead of the IPv6 address. If the local machine has an IPv4 address and the remote machine has an IPv6 address, the local machine must support IPv4 and IPv6 mixed mode. The domain name server must be able to resolve both IPv4 and IPv6 addresses if your environment has both addressing types in a single Linked Mode group.

13 Enter the port numbers to use or accept the default port numbers and click Next.

14 Select the vCenter Server configuration that best describes your setup and click Next.

15 Click Install.

Installation might take several minutes. Multiple progress bars appear during the installation of the selected components.

16 When the installation finishes, click Finish.

You completed the installation of vCenter Server. The Orchestrator client and server components are installed on your system.

**What to do next**

Start the VMware vCenter Orchestrator Configuration service and log in to the Orchestrator configuration interface. Configure Orchestrator using an IPv4 operating system. Orchestrator does not support IPv6 operating systems.

For the detailed procedures, see
1  “Start the Orchestrator Configuration Service,” on page 34
2  “Log In to the Orchestrator Configuration Interface,” on page 34
3  Chapter 7, “Configuring Orchestrator,” on page 33

### Install Orchestrator Standalone

If you install VMware vCenter Server, Orchestrator is already installed on your system. To make Orchestrator available to use, you must only configure it or import a backed up configuration. For production environments and to enhance the scalability of your Orchestrator setup, install Orchestrator on a dedicated Microsoft Windows server.

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.

**Prerequisites**

Verify that your hardware meets the Orchestrator system requirements. See “Hardware Requirements for Orchestrator,” on page 13.
Procedure

1. Download the vCenter Server installation package from the VMware Web site.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use ISO image</td>
<td>The filename is VMware-VIMSetup-xx-4.a.b-yyyy.iso, where a and b are major and minor version, xx is the two-character language code, and yyyy is the build number.</td>
</tr>
<tr>
<td>Use ZIP archive</td>
<td>The filename is VMware-VIMSetup-xx-4.a.b-yyyy.zip, where a and b are major and minor version, xx is the two-character language code, and yyyy is the build number.</td>
</tr>
</tbody>
</table>

2. Extract the files from the archive and browse to the VIMSetup_image\vpx\vCO\ folder.

3. Double-click the vCenterOrchestrator.exe file and click Next.

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

5. Select the Orchestrator installation directory.

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

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accept the default location</td>
<td>Click Next to accept the default installation directory C:\Program Files\VMware\Orchestrator.</td>
</tr>
<tr>
<td>Select a different location</td>
<td>Browse for a different installation directory and click Next.</td>
</tr>
</tbody>
</table>

6. Select the type of installation and click Next.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client</td>
<td>Installs the Orchestrator client application, which allows you to create and edit workflows.</td>
</tr>
<tr>
<td>Server</td>
<td>Installs the Orchestrator platform.</td>
</tr>
<tr>
<td>Client-Server</td>
<td>Installs the Orchestrator client and server.</td>
</tr>
</tbody>
</table>

7. Specify the location for the Orchestrator shortcuts and click Next.

**CAUTION** The name of the shortcuts directory must not contain non-ASCII characters. This is because of a third-party limitation.

8. Click Install to complete the installation process.

9. Click Done to close the installer.

What to do next

Log in to the Orchestrator configuration interface, change the default password, and start configuring Orchestrator. If you used the data migration tool that is included in the vCenter Server 4.1 installation media to export the configuration from your previous Orchestrator installation, you can import your configuration settings. For the detailed procedures, see

- “Log In to the Orchestrator Configuration Interface,” on page 34
- “Change the Default Password,” on page 35
- “Import the Orchestrator Configuration,” on page 58
Install the Orchestrator Client on a 32-Bit Machine

The Orchestrator client is a desktop application that allows you to import packages, run and schedule workflows, and manage user permissions.

You can use the standalone Orchestrator client installer on a 32-bit machine only. For details about installing the Orchestrator client on a 64-bit machine, see “Install Orchestrator Standalone,” on page 21.

Prerequisites
- Log in to the 32-bit machine as an administrator.
- Obtain the standalone Orchestrator client installer.

Procedure
1. Double-click the vCenter Orchestrator Client distribution file and click Next.
   The filename is vCenterOrchestratorClient-4.a.b.-yyy.exe, where a and b are major and minor version and yyy is the build number.

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

3. Select the Orchestrator installation directory.

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

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accept the default location</td>
<td>Click Next to accept the default installation directory C:\Program Files\VMware\Orchestrator.</td>
</tr>
<tr>
<td>Select a different location</td>
<td>Browse for a different installation directory and click Next.</td>
</tr>
</tbody>
</table>

4. Select the Client type of installation and click Next.
5. Specify the location for the Orchestrator shortcuts and click Next.

   ! CAUTION The name of the shortcuts directory must not contain non-ASCII characters. This is because of a third-party limitation.

6. Review the summary and click Next.
7. Click Install to complete the installation process.
8. Click Done to close the installer.

The Orchestrator client component is installed on your system.

What to do next
You can log in to the Orchestrator client interface and perform general administration tasks.
Upgrading to Orchestrator 4.1 and Migrating the Orchestrator Data

When you upgrade vCenter Orchestrator with vCenter Server, you can install vCenter Server on a new machine. You might want to do this to move from a 32-bit to a 64-bit architecture.

The vCenter Server 4.1 installation media include a data migration tool that you can use to migrate configuration data from the original vCenter Server machine to the new machine. For detailed instructions about migrating the vCenter Server configuration and database, see the vSphere Upgrade Guide.

This chapter includes the following topics:
- “Upgrading an Orchestrator Instance Running on a 32-Bit Machine,” on page 25
- “Upgrading an Orchestrator Instance Running on a 64-Bit Machine,” on page 29

Upgrading an Orchestrator Instance Running on a 32-Bit Machine

If vCenter Orchestrator 4.0.x is installed on the same 32-bit machine as vCenter Server 4.0.x, you can use the data migration tool to back up the existing configuration data for Orchestrator and vCenter Server.

The Orchestrator configuration data that you can migrate with the tool includes the following items:
- Network configuration settings
- LDAP connection data
- Database connection data
- SSL certificates
- Licenses
- vCenter plug-in configuration data
- Mail plug-in configuration data
- SSH plug-in configuration data

The Orchestrator database is not migrated. Your new Orchestrator instance accesses the existing database if it is running on a dedicated database server. If you are upgrading from vCenter Orchestrator 4.0, you must update the database from the Database tab of the Orchestrator configuration interface.

If your Orchestrator database is local to the Orchestrator server, it becomes inaccessible after the configuration backup because the 64-bit machine uses the IP address and host name of the source machine. You must set up a new database and configure the database connection from the Database tab of the Orchestrator configuration interface.
Back Up the Orchestrator Configuration Data

Use the data migration tool that is included in the vCenter Server 4.1 installation media to back up the existing Orchestrator configuration and restore it to a new Orchestrator instance.

Migrating Orchestrator configuration settings by using the data migration tool is only possible when Orchestrator is installed silently with vCenter Server. For instructions about migrating configuration settings for a standalone Orchestrator instance, see “Export the Orchestrator Configuration,” on page 57 and “Import the Orchestrator Configuration,” on page 58.

For detailed information about backing up and restoring the existing vCenter Server database and configuration, see the vCenter Sphere Upgrade Guide.

Prerequisites

- Log in to the 32-bit source machine as an administrator.
- Verify that vCenter Orchestrator 4.0 or an update release is installed and configured.
- Stop the VMware vCenter Orchestrator Configuration and VMware vCenter Orchestrator Server services.

Procedure

1. Download the vCenter Server installation package from the VMware Web site.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use ISO image</td>
<td>The filename is VMware-VIMSetup-xx-4.a.b-yyyy.iso, where a and b are major and minor version, xx is the two-character language code, and yyyy is the build number.</td>
</tr>
<tr>
<td>Use ZIP archive</td>
<td>The filename is VMware-VIMSetup-xx-4.a.b-yyyy.zip, where a and b are major and minor version, xx is the two-character language code, and yyyy is the build number.</td>
</tr>
</tbody>
</table>

2. Extract the files from the archive and in the C:\install_directory\ directory, double-click the autorun.exe file.

3. When the vCenter Server Installer page appears, click Explore media.

4. Locate and open the datamigration folder.

5. Extract the files from the datamigration.zip archive to a writeable filesystem (for example, datamigration folder) on the source machine.

6. Run the backup script of the data migration tool.
   - Run the MS-DOS cmd command.
   - Navigate to the datamigration folder.
   - At the command prompt, type backup.bat and press Enter.

   The script checks whether vCenter Server and vCenter Update Manager are installed and meet the migration prerequisites. The script then proceeds to the backup of the vCenter Orchestrator configuration.

7. Respond to the prompts and wait for the script to complete.
   - If the script fails, check the generated backup.log file that is located in the datamigration\logs folder.

The existing Orchestrator configuration is successfully exported. The file that stores the system settings is named vco.backup.vmoconfig and is located in the datamigration\data\vco folder.
**What to do next**

Back up any standard Orchestrator elements that you modified. During the database upgrade, elements with a higher version number silently overwrite the existing elements. See “Back Up Modified and Custom Orchestrator Elements,” on page 27.

**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.

**Install Orchestrator with vCenter Server on a 64-Bit Machine and Import the Configuration Data**

When you install VMware vCenter Server, Orchestrator is silently installed on your system as an additional component. Use the data migration tool to launch the vCenter Server installer, install vCenter Orchestrator 4.1, and import the configuration from your previous Orchestrator installation.

For detailed information about installing vCenter Server 4.1 and restoring the existing vCenter Server database and configuration, see the vCenter Sphere Upgrade Guide.

**Prerequisites**

- Log in to the 64-bit machine as an administrator.
- Use the same IP address and host name for the 64-bit machine that you used for the source 32-bit machine.
- Copy the folder in which you extracted the files from the datamigration.zip archive to the 64-bit machine.
Procedure

1 Download the vCenter Server installation package from the VMware Web site.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use ISO image</td>
<td>The filename is VMware-VIMSetup-xx-4.a.b-yyyy.iso, where a and b are major and minor version, xx is the two-character language code, and yyyy is the build number.</td>
</tr>
<tr>
<td>Use ZIP archive</td>
<td>The filename is VMware-VIMSetup-xx-4.a.b-yyyy.zip, where a and b are major and minor version, xx is the two-character language code, and yyyy is the build number.</td>
</tr>
</tbody>
</table>

2 Run the install script of the data migration tool to launch the vCenter Server installer.
   a Run the MS-DOS cmd command.
   b Navigate to the datamigration folder you copied from the source machine.
   c At the command prompt, type install.bat and press Enter.
      The script verifies that migration data is present.
   d At the prompt, type the path to the vCenter Server 4.1 install media and press Enter.
      The script launches the vCenter Server installer.

3 Select a language for the installer and click OK.

4 When the Welcome page appears, click Next.

5 Click Next on the End-User Patent Agreement page.

6 Select I agree to the terms in the license agreement and click Next.

7 Choose the type of database to use.

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Install SQL Server 2005 Express instance (for small-scale deployments)</td>
<td>Select this option if you used the bundled SQL Express database on the source machine.</td>
</tr>
<tr>
<td>Use an existing supported database</td>
<td>Select this option to use an existing non-bundled database. Select the DSN that was used for the database on the source machine. Enter the user name and password for the DSN and click Next. If you specify a remote SQL Server database that uses Windows NT authentication, the database user and the logged-in user on the vCenter Server machine must be the same.</td>
</tr>
</tbody>
</table>

A dialog box appears warning that the DSN points to an older version of a repository that must be upgraded.

8 Click Yes to upgrade the database schema.

   The upgraded database is irreversibly incompatible with previous vCenter Server versions.

9 Specify the account for the vCenter Service to run in.
   - Click Next to use the SYSTEM account. You cannot use the SYSTEM account if you are using Windows authentication for SQL Server.
   - Deselect Use SYSTEM Account, accept the default Administrator account name and password, and click Next.
   - Deselect Use SYSTEM Account and enter a different Administrator account name and password.

10 Either accept the default destination folders or click Change to select another location, and click Next.

   The installation path cannot have commas (,) or periods (.).
11 Enter the port numbers to use or accept the port numbers that were imported from the source vCenter Server installation and click Next.
For a list of required ports, see the ESX and vCenter Server Installation Guide.

12 Select the vCenter Server configuration that best describes your setup and click Next.

13 Click Install.
Installation might take several minutes. If the install script fails, check the generated backup.log file that is located in the datamigration\logs folder.

14 When the installation finishes, click Finish.
The data migration tool restores the backed up configuration data and starts the vCenter Server service.

- vCenter Server and the Orchestrator client and server components are installed.
- The configuration settings from your previous Orchestrator installation are imported.

What to do next
Start the VMware vCenter Orchestrator Configuration service and log in to the Orchestrator configuration interface. If you migrated from vCenter Orchestrator 4.0, you must update the Orchestrator database.
If your Orchestrator database is local to the 32-bit Orchestrator server, it is inaccessible after the configuration backup. You must set up a new database and configure the database connection from the Database tab in the Orchestrator configuration interface.
For the detailed procedures, see
- “Start the Orchestrator Configuration Service,” on page 34
- “Log In to the Orchestrator Configuration Interface,” on page 34
- “Configure the Database Connection,” on page 45

Upgrading an Orchestrator Instance Running on a 64-Bit Machine
If vCenter Orchestrator 4.0.x is installed on the same 64-bit machine as vCenter Server 4.0.x, you cannot perform an in-place upgrade of Orchestrator by using the data migration tool.
To upgrade to vCenter Orchestrator 4.1, you must export the Orchestrator configuration settings, uninstall the existing Orchestrator instance, run the 64-bit Orchestrator installer and import the configuration settings.
For the detailed procedures, see
1 “Export the Orchestrator Configuration,” on page 57
2 Chapter 6, “Uninstall Orchestrator,” on page 31
3 “Install Orchestrator Standalone,” on page 21
4 “Import the Orchestrator Configuration,” on page 58
Uninstall 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 57.

Back up custom workflows and plug-ins.

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 is uninstalled from your system.
VMware vCenter Orchestrator Web Configuration is installed silently with VMware vCenter Server. This is the tool you use 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:

- “Start the Orchestrator Configuration Service,” on page 34
- “Log In to the Orchestrator Configuration Interface,” on page 34
- “Change the Default Password,” on page 35
- “Revert to the Default Password for Orchestrator Configuration,” on page 35
- “Configure the Network Connection,” on page 36
- “Change the Default Configuration Ports on the Orchestrator Client Side,” on page 38
- “Import the vCenter Server SSL Certificate,” on page 39
- “Configuring LDAP Settings,” on page 39
- “Password Encryption and Hashing Mechanism,” on page 45
- “Configure the Database Connection,” on page 45
- “Server Certificate,” on page 47
- “Configure the Default Plug-Ins,” on page 50
- “Access Rights to Orchestrator Server,” on page 54
- “Import the vCenter Server License,” on page 54
- “Start the Orchestrator Server,” on page 55
- “Export the Orchestrator Configuration,” on page 57
- “Import the Orchestrator Configuration,” on page 58
- “Configure the Maximum Number of Events and Runs,” on page 59
- “Install an Application,” on page 59
- “Import the Plug-In Licenses,” on page 60
- “Change the Web View SSL Certificate,” on page 60
- “Define the Server Log Level,” on page 61
Start the Orchestrator Configuration Service

The VMware vCenter Orchestrator Configuration service startup type is set to Manual by default. You must start it manually before you try to access the Orchestrator configuration interface and after you reboot the Orchestrator server.

If you installed Orchestrator standalone, the Orchestrator Configuration service is already started.

Procedure

1. Right-click My Computer on your desktop and select Manage.
2. In the Computer Management dialog box, expand Services and Applications and select Services.
3. Locate VMware vCenter Orchestrator Configuration on the list and check its status.
4. If the status is not set, right-click VMware vCenter Orchestrator Configuration and select Start.

The Orchestrator Configuration service is now running and Orchestrator configuration interface is available for use.

What to do next

You can log in to the Orchestrator configuration interface and start the process of configuring Orchestrator.

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 cannot view the Orchestrator configuration shortcut if you are logged in to the Orchestrator server machine as a different user than the user who installed Orchestrator. To access the configuration interface, go to install_directory\Orchestrator\configuration and double-click the VMOConfiguration shortcut.

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
   
   You can change the password after you log in for the first time.
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.

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>If you installed Orchestrator with the vCenter Server installer</td>
<td>Go to <code>install_directory\VMware\Infrastructure\Orchestrator\configuration\jetty\etc</code>.</td>
</tr>
<tr>
<td>If you installed the standalone version of Orchestrator</td>
<td>Go to <code>install_directory\VMware\Orchestrator\configuration\jetty\etc</code>.</td>
</tr>
</tbody>
</table>

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 that the Orchestrator client interface uses to communicate to the server is not set automatically. To change this, you must configure the network settings used by Orchestrator.

Prerequisites

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 the IP address remains 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 IP address to which you want to bind the Orchestrator server.

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

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 36.

5 Click Apply changes.

What to do next

Click SSL Certificate to load the vCenter Server 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 the Orchestrator JBoss application server uses. The ports are set with a default value, but you can change these values at any time. When you make the changes, verify that all ports are free on your host and, if necessary, open these ports on required firewalls.

Default Configuration Ports

To provide the Orchestrator service, you must set the default ports and configure your firewall to allow incoming TCP connections.

NOTE Other ports might be required if you are using custom plug-ins.
### Table 7-1. VMware vCenter Orchestrator Default Configuration Ports

<table>
<thead>
<tr>
<th>Port</th>
<th>Number</th>
<th>Protocol</th>
<th>Source</th>
<th>Target</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lookup port</td>
<td>8230</td>
<td>TCP</td>
<td>Orchestrator client</td>
<td>Orchestrator server</td>
<td>The main port to communicate with the Orchestrator server (JNDI port). All other ports communicate with the Orchestrator client through this port. It is part of the JBoss application server infrastructure.</td>
</tr>
<tr>
<td>Command port</td>
<td>8240</td>
<td>TCP</td>
<td>Orchestrator client</td>
<td>Orchestrator server</td>
<td>The application communication port (RMI container port) used for loading the Orchestrator client remotely. It is part of the JBoss application server infrastructure.</td>
</tr>
<tr>
<td>Messaging port</td>
<td>8250</td>
<td>TCP</td>
<td>Orchestrator client</td>
<td>Orchestrator server</td>
<td>The Java messaging port used for dispatching events. It is part of the JBoss application server infrastructure.</td>
</tr>
<tr>
<td>Data port</td>
<td>8244</td>
<td>TCP</td>
<td>Orchestrator client</td>
<td>Orchestrator server</td>
<td>The port used for accessing all Orchestrator data models, such as workflows and policies. It is part of the JBoss application server infrastructure.</td>
</tr>
<tr>
<td>HTTP server port</td>
<td>8280</td>
<td>TCP</td>
<td>End-user Web browser</td>
<td>Orchestrator server</td>
<td>The port used by the Orchestrator server to connect to the Web view front end through HTTP.</td>
</tr>
<tr>
<td>HTTPS server port</td>
<td>8281</td>
<td>TCP</td>
<td>End-user Web browser</td>
<td>Orchestrator server</td>
<td>The SSL secured HTTP protocol used to connect to the Web view front end and to communicate with the vCenter Server API.</td>
</tr>
<tr>
<td>Web configuration HTTP access port</td>
<td>8282</td>
<td>TCP</td>
<td>End-user Web browser</td>
<td>Orchestrator configuration</td>
<td>The access port for the Web UI of Orchestrator configuration.</td>
</tr>
<tr>
<td>Web configuration HTTPS access port</td>
<td>8283</td>
<td>TCP</td>
<td>End-user Web browser</td>
<td>Orchestrator configuration</td>
<td>The SSL access port for the Web UI of Orchestrator configuration. <strong>Note</strong>: To enable the HTTPS connection, configure Jetty to use SSL. See <a href="#">Jetty Documentation, Configuring SSL</a>.</td>
</tr>
</tbody>
</table>

### External Communication Ports

You must configure your firewall to allow outgoing connections so that Orchestrator can communicate with external services.

### Table 7-2. VMware vCenter Orchestrator External Communication Ports

<table>
<thead>
<tr>
<th>Port</th>
<th>Number</th>
<th>Protocol</th>
<th>Source</th>
<th>Target</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LDAP</td>
<td>389</td>
<td>TCP</td>
<td>Orchestrator server</td>
<td>LDAP server</td>
<td>The lookup port of your LDAP Authentication server.</td>
</tr>
<tr>
<td>LDAP using SSL</td>
<td>636</td>
<td>TCP</td>
<td>Orchestrator server</td>
<td>LDAP server</td>
<td>The lookup port of your secure LDAP Authentication server.</td>
</tr>
<tr>
<td>LDAP using Global Catalog</td>
<td>3268</td>
<td>TCP</td>
<td>Orchestrator server</td>
<td>Global Catalog server</td>
<td>The port to which Microsoft Global Catalog server queries are directed.</td>
</tr>
<tr>
<td>SQL Server</td>
<td>1433</td>
<td>TCP</td>
<td>Orchestrator server</td>
<td>Microsoft SQL Server</td>
<td>The port used to communicate with the Microsoft SQL Server or SQL Server Express instances that are configured as the Orchestrator database.</td>
</tr>
<tr>
<td>Oracle</td>
<td>1521</td>
<td>TCP</td>
<td>Orchestrator server</td>
<td>Oracle DB Server</td>
<td>The port used to communicate with the Oracle Database Server that is configured as the Orchestrator database.</td>
</tr>
</tbody>
</table>
Table 7-2. VMware vCenter Orchestrator External Communication Ports (Continued)

<table>
<thead>
<tr>
<th>Port</th>
<th>Number</th>
<th>Protocol</th>
<th>Source</th>
<th>Target</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SMTP Server port</td>
<td>25</td>
<td>TCP</td>
<td>Orchestrator server</td>
<td>SMTP Server</td>
<td>The port used for email notifications.</td>
</tr>
<tr>
<td>vCenter Server API port</td>
<td>443</td>
<td>TCP</td>
<td>Orchestrator server</td>
<td>vCenter Server</td>
<td>The vCenter Server API communication port used by Orchestrator to obtain virtual infrastructure and virtual machine information from the orchestrated vCenter Server instances.</td>
</tr>
</tbody>
</table>

Internal JBoss Ports

Internal JBoss Server ports do not need to be added to the firewall exceptions.

Table 7-3. Internal JBoss Server Ports

<table>
<thead>
<tr>
<th>Port Number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>3455</td>
<td>RMI server registry invoker</td>
</tr>
<tr>
<td>3873</td>
<td>EJB3 and AOP remoting connector</td>
</tr>
<tr>
<td>4445</td>
<td>JBoss pooled invoker</td>
</tr>
<tr>
<td>4446</td>
<td>Remoting server service connector</td>
</tr>
<tr>
<td>8083</td>
<td>Dynamic class and resource loader</td>
</tr>
</tbody>
</table>

Change the Default Configuration Ports on the Orchestrator Client Side

If 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.

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>If you installed Orchestrator with the vCenter Server installer</td>
<td>Go to install_directory\VMware\Infrastructure\Orchestrator\apps.</td>
</tr>
<tr>
<td>If you installed the standalone version of Orchestrator</td>
<td>Go to install_directory\VMware\Orchestrator\apps.</td>
</tr>
</tbody>
</table>

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 Server SSL Certificate**

The Orchestrator configuration interface uses a secure connection to communicate with vCenter Server. 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 Server SSL certificate in Orchestrator from a URL address or file.

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Import from URL</strong></td>
<td>Specify the URL of the vCenter Server:</td>
</tr>
<tr>
<td></td>
<td><strong>https://your_vcenter_server_IP_address</strong></td>
</tr>
<tr>
<td><strong>Import from file</strong></td>
<td>Obtain the vCenter Server certificate file. The file is usually available at the following locations:</td>
</tr>
<tr>
<td></td>
<td>- C:\Documents and Settings\AllUsers\ApplicationData\VMware\VMwareVirtualCenter\SSL\rui.crt</td>
</tr>
<tr>
<td></td>
<td>- /etc/vmware/ssl/rui.crt</td>
</tr>
</tbody>
</table>

5. Click **Import**.

A message confirming that the import is successful appears.

6. Repeat the steps for each vCenter Server instance that you want to add to the Orchestrator server.

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 to a vCenter Server instance, you must return to the **SSL Certificate** tab on the **Network** tab and import the corresponding vCenter Server SSL certificate.

**Configuring LDAP Settings**

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

1. **Generate the LDAP Connection URL** on page 40

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

2. **Import the LDAP Server SSL Certificate** on page 41

   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.

3. **Specify the Browsing Credentials** on page 42

   Orchestrator must read your LDAP structure to inherit its properties. You can specify the credentials that Orchestrator uses to connect to an LDAP server.
4 Define the LDAP User and Group Lookup Paths on page 42
You can define the users and groups lookup information.

5 Define the LDAP Search Options on page 44
You can customize the LDAP search queries and make searching in LDAP more effective.

6 Common Active Directory LDAP Errors on page 44
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 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, eDirectory, 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 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.

5 (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.

6 In the Port text box, type the value for the lookup port of your LDAP server.

**Note** Orchestrator supports the 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.

7 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 for browsing 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.
8 (Optional) Select **Use SSL** 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 41.

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

The LDAP server lookup 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: Values and Resulting LDAP Connection URL Addresses**

Examples of the values that you enter in the required fields and the resulting LDAP connection URL.

- **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 42.

**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, eDirectory, 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.
- If you are using LDAPS, Windows 2003 or 2008, and AD, verify that the **LDAP Server Signing Requirements** group policy is disabled 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**

Ensure that you have a working LDAP service in your infrastructure and have generated the LDAP connection URL.

**Procedure**

1. Log in to the Orchestrator configuration interface as **vmware**.
2. Click **LDAP**.
3. Specify the primary and secondary LDAP hosts, the lookup port of the LDAP server, and the root element.
4. Type a valid user name (LDAP string) in the **User name** text box for a user who has browsing permissions on your LDAP server.
   
   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 Sun and eDirectory. Do not use spaces between the comma and the next identifier.
   - Principal name format: **user@company.org**.
   - NetBEUI format: **COMPANY\user**.
5. In the **Password** text box, type the password for the user name you entered in Step 4.

Orchestrator uses the 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 User and Group 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. Specify the primary and secondary LDAP hosts, the lookup port of the LDAP server, the root element, and the browsing credentials.
4. 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 that Orchestrator follows to find the account or group in a subdomain.
5. 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.
6. 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.
   
   **IMPORTANT** In eDirectory installations, only the eDirectory administrator can see users or user groups that have administration rights. If you are using an eDirectory LDAP server, and you log in to Orchestrator as a member of the vCO Admin group but you are not the eDirectory administrator, you can create users or user groups with administration rights, but you cannot see those users. This problem does not apply to other LDAP servers.
7. 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 part of 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>
<thead>
<tr>
<th>Error</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>525</td>
<td>The user is not found.</td>
</tr>
<tr>
<td>52e</td>
<td>The user credentials are not valid.</td>
</tr>
<tr>
<td>530</td>
<td>The user is not allowed to log in at this time.</td>
</tr>
<tr>
<td>531</td>
<td>The user is not allowed to log in to this workstation.</td>
</tr>
<tr>
<td>532</td>
<td>The password has expired.</td>
</tr>
<tr>
<td>533</td>
<td>This user account has been disabled.</td>
</tr>
<tr>
<td>701</td>
<td>This user account has expired.</td>
</tr>
</tbody>
</table>
Table 7-4. Common Active Directory Authentication Errors (Continued)

<table>
<thead>
<tr>
<th>Error</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>773</td>
<td>The user must reset their password.</td>
</tr>
<tr>
<td>775</td>
<td>The user account has been locked.</td>
</tr>
</tbody>
</table>

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 7-5. Encryption and Hashing Algorithms in Orchestrator

<table>
<thead>
<tr>
<th>Algorithm</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password Based Encryption (part of Java 2 SDK 1.4)</td>
<td>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.</td>
</tr>
<tr>
<td>Message Digest 5 algorithm</td>
<td>Generates a 128-bit cryptographic message digest value, usually expressed as a 32 digit hexadecimal number.</td>
</tr>
<tr>
<td>Data Encryption Standard</td>
<td>Applies a 56-bit key to each 64-bit block of data.</td>
</tr>
</tbody>
</table>

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 18.
- For a list of database connection parameters, see “Database Connection Parameters,” on page 46.
- 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** Orchestrator supports Oracle, SQL Server, and SQL Server Express.

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.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Install the database</td>
<td>Builds a new table structure for the Orchestrator database.</td>
</tr>
<tr>
<td>Update the database</td>
<td>Uses the database from your previous Orchestrator installation and updates</td>
</tr>
<tr>
<td></td>
<td>the table structure.</td>
</tr>
</tbody>
</table>

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, you must 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 might vary.

**Table 7-6. Database Connection Parameters**

<table>
<thead>
<tr>
<th>Connection Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td>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 <code>db_owner</code> rights.</td>
</tr>
<tr>
<td>Password</td>
<td>The password for the user name you entered.</td>
</tr>
<tr>
<td>Database host IP address or DNS name</td>
<td>The database server IP address or DNS name.</td>
</tr>
<tr>
<td>Port</td>
<td>The database server port that allows communication to your database.</td>
</tr>
<tr>
<td>Database name</td>
<td>The full unique name of your database. The database name is specified by the <code>SERVICE_NAMES</code> parameter in the initialization parameter file.</td>
</tr>
<tr>
<td>Instance name (if any)</td>
<td>The name of the database instance that can be identified by the <code>INSTANCE_NAME</code> parameter in the database initialization parameter file.</td>
</tr>
<tr>
<td>Domain (SQL Server only)</td>
<td>To use Windows authentication, specify the domain name of the SQL Server machine, for example <code>company.org</code>.</td>
</tr>
<tr>
<td></td>
<td>To use SQL authentication, leave this text box blank.</td>
</tr>
<tr>
<td>Use Windows authentication mode (NTLMv2)</td>
<td>Select to send NTLMv2 responses when using Windows authentication.</td>
</tr>
<tr>
<td></td>
<td>This option is valid only for SQL Server.</td>
</tr>
</tbody>
</table>

### 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.
Check the connection type.

**Configure SQL Server Express to Use with Orchestrator**

You can use Microsoft SQL Server Express in small-scale environments. Orchestrator can work with SQL Server Express when the deployment does not exceed 5 hosts and 50 virtual machines.

To use SQL Server Express with Orchestrator, you must configure the database to enable TCP/IP.

**Procedure**

1. Log in as an administrator to the machine on which SQL Server Express is installed.
2. Click **Start > All Programs > Microsoft SQL Server 2008 R2 > Configuration Tools > SQL Server Configuration Manager**.
3. Expand in the list on the left.
4. Click **Protocols for SQLEXPRESS**.
5. Right-click **TCP/IP** and select **Enable**.
6. Right-click **TCP/IP** and select **Properties**.
7. Click the **IP Addresses** tab.
8. Under **IP1**, **IP2**, and **IPAll**, set the **TCP Port** value to **1433**.
9. Click **OK**.
10. Click on the left.
11. Restart the SQL Server.

**What to do next**

Configure the Orchestrator database connection parameters.

**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.

1. Import a Server Certificate on page 48
   You can import a server certificate and use it with Orchestrator.
2. Create a Self-Signed Server Certificate on page 48
   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.
3. Obtain a Server Certificate Signed by a Certificate Authority on page 49
   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.
4 Export a Server Certificate on page 49
   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.

5 Change a Self-Signed Server Certificate on page 50
   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](image)
   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\VSOPPluginInstallationVersion.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 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.

<table>
<thead>
<tr>
<th>Text box</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SMTP host</td>
<td>Enter the IP address or domain name of your SMTP server.</td>
</tr>
<tr>
<td>SMTP port</td>
<td>Enter a port number to match your SMTP configuration. The default SMTP port is 25.</td>
</tr>
</tbody>
</table>
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 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 Server SSL Certificate,” on page 39.

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

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.

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.

Specify the method you use to manage user access on the vCenter Server host.

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Share a unique session</strong></td>
<td>Select this option to allow Orchestrator to create only one connection to vCenter Server. Enter the credentials of a user who is a vCenter Server administrator.</td>
</tr>
<tr>
<td><strong>Session per user</strong></td>
<td>Select this option if your vCenter Server is in an Active Directory domain. Verify that the user has the necessary permissions to perform the required operations. CAUTION Each user who logs in Orchestrator creates a new session to vCenter Server. This can rapidly strain CPU, memory and bandwidth.</td>
</tr>
</tbody>
</table>

Click **Apply changes**.

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

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.

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>If you installed Orchestrator with the vCenter Server installer</strong></td>
<td>Go to <code>install_directory\VMware\Infrastructure\Orchestrator\app-server\server\vmo\plugins</code>.</td>
</tr>
<tr>
<td><strong>If you installed the standalone version of Orchestrator</strong></td>
<td>Go to <code>install_directory\VMware\Orchestrator\app-server\server\vmo\plugins</code>.</td>
</tr>
</tbody>
</table>

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. In the Orchestrator client, click the Packages view.
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.

### Access Rights to Orchestrator Server

The type of vCenter Server license you apply in the Orchestrator configuration interface determines whether you get read-only or full access to the Orchestrator server capabilities.

#### Table 7-7. Orchestrator Server Modes

<table>
<thead>
<tr>
<th>vCenter License Edition</th>
<th>vCenter Orchestrator Mode</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standard</td>
<td>Server</td>
<td>You are granted full read and write privileges to all Orchestrator elements. You can run and edit workflows.</td>
</tr>
<tr>
<td>Foundation</td>
<td>Player</td>
<td>You are granted read privileges on all Orchestrator elements. You can run workflows but you cannot edit them.</td>
</tr>
<tr>
<td>Essentials</td>
<td>Player</td>
<td>You are granted read privileges on all Orchestrator elements. You can run workflows but you cannot edit them.</td>
</tr>
<tr>
<td>Evaluation</td>
<td>Server</td>
<td>You are granted full read and write privileges to all Orchestrator elements. You can run and edit workflows.</td>
</tr>
</tbody>
</table>

**NOTE** All predefined workflows are locked as read-only by design. To edit a standard workflow, you must duplicate the workflow and make changes to the duplicated workflow.

### 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 Server SSL Certificate,” on page 39.

#### 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 process is reversible as you can always use the Uninstall vCO server from service option.

Prerequisites

- If you installed Orchestrator silently with vCenter Server, verify that your system has at least 4GB of RAM and that the database is running on a dedicated server. The Orchestrator server might not start if your system does not meet this requirement.
- If you installed Orchestrator standalone, verify that your 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 Log in to the Orchestrator configuration interface as vmware.

2 Click Startup Options.

3 Click Install vCO server as service.

The Orchestrator server is installed as a Windows service.

4 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
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 57.

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 follows:

   ```
   -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). See “Activate the Service Watchdog Utility,” on page 56.

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 57.

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 7-8. Settings Not Saved During Configuration Export

<table>
<thead>
<tr>
<th>File</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>certificate</td>
<td>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.</td>
</tr>
<tr>
<td>licenses</td>
<td>Manually imported licenses are not exported. They are stored in the Orchestrator database.</td>
</tr>
<tr>
<td>server</td>
<td>The server configuration is reset to Unknown. You must install the Orchestrator server as a Windows service again.</td>
</tr>
</tbody>
</table>

Table 7-9. Settings Saved During Configuration Export

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

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 a workflow three times, three workflow tokens are created. The three tokens appear in the Orchestrator client below the 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. See `vCenter Orchestrator Developer’s Guide`.
8. Click `Apply changes`.

Install an Application

An application is a set of plug-ins and packages. Because an Orchestrator installation contains only a few pre-defined plug-ins, you can install new plug-ins to extend basic functions, as they become available, or as you develop them.

Prerequisites

Obtain the `.vmoapp` file containing the application.

Procedure

1. Log in to the Orchestrator configuration interface as `vmware`.
2 On the General tab, click Install Application.
3 Browse to select the .vmoapp file to install.
4 Click Install.

What to do next
Every time you install an application, a validation is made on the server configuration. In most cases, you must perform additional configuration steps on a tab that the new application adds to the Orchestrator configuration interface.

Import the Plug-In Licenses
The set of plug-ins that Orchestrator includes does not require a license. If you add a plug-in that requires a license, you must import it in the Orchestrator configuration interface.

Procedure
1 Log in to the Orchestrator configuration interface as vmware.
2 Click Licenses.
3 On the Licenses tab, click Plug-in Licenses.
4 In the Serial number text box, type your plug-in license key.
5 Click Apply changes.

What to do next
To view details, click the name of the imported license.

Change the Web View SSL Certificate
Orchestrator provides an SSL certificate that controls user access to Web views. You can configure Orchestrator to use a different SSL certificate to control access to Web views. For example, 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 following Orchestrator application server configuration file in an editor.

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>If you installed the standalone version of Orchestrator</td>
<td>Go to <code>install_directory\VMware\Orchestrator\app-server\server\vmo\deploy\jboss-deploy-tomcat\jbossweb-tomcat55.sar\server.xml</code></td>
</tr>
<tr>
<td>If the vCenter Server installed Orchestrator</td>
<td>Go to <code>install_directory\VMware\Infrastructure\Orchestrator\app-server\server\vmo\deploy\jboss-deploy-tomcat\jbossweb-tomcat55.sar\server.xml</code></td>
</tr>
</tbody>
</table>
3 Find the following entry at line 44 in the server.xml file.

```xml
<!-- 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.

```xml
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. The default server log level is **INFO**. Changing the log level affects any new messages that the server writes to the server log and the number of active connections to the database.

![CAUTION](image)

**CAUTION** Only set the log level to **DEBUG** or **ALL** to debug a problem. Do not use this setting in a production environment because it can seriously impair performance.

**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.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FATAL</td>
<td>Only fatal errors are written to the log file.</td>
</tr>
<tr>
<td>ERROR</td>
<td>Errors and fatal errors are written to the log file.</td>
</tr>
<tr>
<td>WARN</td>
<td>Warnings, errors, and fatal errors are written to the log file.</td>
</tr>
<tr>
<td>INFO</td>
<td>Information, warnings, errors, and fatal errors are written to the log file.</td>
</tr>
<tr>
<td>DEBUG</td>
<td>Debug information, information messages, warnings, errors, and fatal errors are written to the log file.</td>
</tr>
<tr>
<td>ALL</td>
<td>Events are not filtered. All events are written to the log file.</td>
</tr>
<tr>
<td>OFF</td>
<td>No entries are written to the log file and no log updates are made.</td>
</tr>
</tbody>
</table>

**NOTE** The log contains 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 log files.
The new log level is applied to any new messages that the server generates, without restarting the server. The logs are stored in `install_directory\app-server\server\vmo\log`. 
Where to Go From Here

When you have installed and configured vCenter Orchestrator, you can use Orchestrator to automate frequently repeated processes related to the management of the virtual environment.

- Log in to the Orchestrator client, run, and schedule workflows on the vCenter Server inventory objects or other objects that Orchestrator accesses through its plug-ins.
- Publish the weboperator Web view and provide browser access to Orchestrator workflows to users and user groups.
- Set up the user permissions on Orchestrator objects.
- Duplicate and modify the standard Orchestrator workflows and write your own actions and workflows to automate operations in vCenter Server.
- Develop plug-ins, Web services, and Web views to extend the Orchestrator platform.

For information about features and instructions about using and maintaining Orchestrator, see the vCenter Orchestrator Administration Guide.

For guidance with advanced development tasks and extending the Orchestrator platform, see the vCenter Orchestrator Developer’s Guide.
Index

A
authorizations 12
availability 17

C
certificate database 49, 50
changing the Orchestrator Lookup port 38
check-pointing 9
configuration
config files 57
database connection 45, 46
default plug-ins 50
export configuration settings 57
import configuration settings 58
LDAP settings 42
network connection 36
configuration maximums 17

D
data migration tool
back up customized elements 27
data migration 25
export configuration settings 26
import configuration settings 27
database
connection parameters 45, 46
installation 18
Oracle 18
server size 18
setup 18
SQL Server 18
SQL Server Express 18
default password 35
default ports
command port 36
data port 36
HTTP port 36
HTTPS port 36
JBoss server ports 36
LDAP port 36
LDAP with Global Catalog 36
LDAP with SSL 36
lookup port 36
messaging port 36
Oracle port 36
SMTP port 36
SQL Server port 36
vCenter API port 36
Web configuration HTTP access port 36
Web configuration HTTPS access port 36
deprecated features 12
dereference links 44
DES 45

E
encryption 45
events 59

F
feedback 7
filter attributes 44

H
hashing 45

I
i18n support 14
ignore referrals 44
installing Orchestrator
vCenter Orchestrator client installer 23
vCenter Orchestrator server installer 21
vCenter Server installer 19
internationalization 14
IPv4 19
IPv6 19

L
LDAP
browsing credentials 42
connection URL 40
LDAP Server Signing Requirements 41
lookup paths 42
SSL certificate 41
LDAP errors
525 44
52e 44
530 44
531 44
532 44
533 44
service watchdog utility
  timeout parameter 56
  troubleshooting server restarts 56
services
  starting 34, 55
  VMware vCenter Orchestrator Configuration 34
  VMware vCenter Orchestrator Server 55
setup guidelines
  directory services 18
  LDAP server 18
  vCenter Server 17
  SMTP connection 51
SQL authentication type 46
SQL Express, configuring SQL Express 47
SSL certificate 39
support 7
system requirements
  directory services 13
  hardware 13
  operating systems 13
  supported browsers 14
  supported databases 14

T
timeouts 44

U
uninstalling 31
updated information 5
upgrading Orchestrator 19
user roles 10

V
versioning 9
VMware vCenter Orchestrator Server, installing
  as Windows service 55

W
watchdog utility 56
Web views, change SSL certificate 60
what to do next 63
workflow engine 9

701 44
773 44
775 44
license
  importing plug-in licenses 60
  importing vCenter Server license 54
  Orchestrator server access rights 54
load balancing 51
login 34

M
MD5 45

N
non-ASCII characters 14, 21, 45

O
OGNL expressions 12
  Orchestrator architecture 11
  Orchestrator installed on a 32-bit machine 25
  Orchestrator installed on a 64-bit machine 29
  Orchestrator overview 9

P
password 35
PBE 45
  persistence 9
plug-ins
  installing an application 59
  Mail plug-in 51
  removing a plug-in 53
  SSH plug-in 52
  vCenter Server plug-in 52
policies 12
  policy engine 9

R
  runs 59

S
  scalability 17
  scripting engine 9
  security 9
server certificate
  CA-signed 47, 49
  exporting 48, 49
  importing 48
  removing 50
  self-signed 47, 48
server log
  exporting 61
  log level 61