Using the VMware vCenter Orchestrator Appliance

vCenter Orchestrator 5.1

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

Using the vCenter Orchestrator Appliance 5

1 Introduction to VMware vCenter Orchestrator 7
   Key Features of the Orchestrator Platform 7
   Orchestrator User Types and Related Responsibilities 8
   Orchestrator Architecture 9
   Orchestrator Plug-Ins 10

2 Overview of the Orchestrator Appliance 11
   Download and Deploy the Orchestrator Appliance 12
   Power On the Orchestrator Appliance and Log In to the Appliance Web Console 13

3 Configuring the Orchestrator Appliance 15
   Log In to the Orchestrator Appliance Web Console 15
   Change the Default Root Password 16
   Enable or Disable SSH Administrator Login on the vCenter Orchestrator Appliance 16
   Configure Network Settings for the Orchestrator Appliance 16
   Upgrading the Orchestrator Appliance 17
      Check the Orchestrator Appliance Version Status 17
      Configure the Orchestrator Appliance for Updates 18
      Install Available Updates Manually 18

4 Configuring vCenter Orchestrator 21
   Log In to the Orchestrator Configuration Interface 22
   Import a vCenter Server SSL Certificate and License 22
   Install and Configure the vCenter Server Plug-In 23
      Install the vCenter Server Plug-In 24
      Import the vCenter Server SSL Certificate 24
      Configure the vCenter Server 5.1 Plug-In 25
   Selecting the Authentication Type 26
      Configuring vCenter Single Sign On Settings 26
      Configuring LDAP Settings 29
   Orchestrator Database Setup 34
      Import the Database SSL Certificate 35
      Configure the Database Connection 36
   Changing SSL Certificates 37
      Generate a New Certificate 37
      Install a Certificate from a Certificate Authority 38
      Change the Certificate of the Orchestrator Appliance Management Site 39
      Change the Web Views SSL Certificate 39
      Change the SSL Certificate of the Orchestrator Configuration Interface 40
5 The Orchestrator Client and Web Operator  43
   Log In to the Orchestrator Client  43
   Log In to the Orchestrator Web Operator  44
   Download and Install the Orchestrator Client  45

Index  47
Using the vCenter Orchestrator Appliance

Using the vCenter Orchestrator Appliance provides information about deploying and using VMware vCenter Orchestrator™ Appliance.

Intended Audience

This information is intended for anyone who wants to use the Orchestrator Appliance. The information is written for experienced Windows or Linux system administrators who are familiar with virtual machine technology and datacenter operations.

For more information about Orchestrator, see http://www.vmware.com/support/pubs/orchestrator_pubs.html.
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 vSphere 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 7
- “Orchestrator User Types and Related Responsibilities,” on page 8
- “Orchestrator Architecture,” on page 9
- “Orchestrator Plug-Ins,” on page 10

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 or REST 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

Users, other workflows, a schedule, or a policy can start workflows.

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 Types and Related Responsibilities

Orchestrator provides different tools and interfaces based on the specific responsibilities of the two global user roles: Administrators and End Users. Orchestrator developers also have administrative rights and are responsible for creating workflows and additional applications.

Users with Full Rights

Administrators

This role has full access to all of the Orchestrator platform capabilities. Basic administrative responsibilities 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 user type 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 automated processes, using Web 2.0 tools.

**Users with Limited Rights**

**End Users**

This role has access to only the Web front end. End users can run and schedule workflows and policies that the administrators or developers make available in a browser by using Web views.

**Orchestrator Architecture**

Orchestrator contains a workflow library and a 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 for 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, the Orchestrator workflows, and the objects it exposes through the Orchestrator client interface, through a Web browser, or through Web services.
Orchestrator Plug-Ins

Plug-ins allow you to use Orchestrator to access and control external technologies and applications. Exposing an external technology in an Orchestrator plug-in allows you to incorporate objects and functions in workflows that access the objects and functions of that external technology.

The external technologies that you can access by using plug-ins can include virtualization management tools, email systems, databases, directory services, and remote control interfaces.

Orchestrator provides a set of standard plug-ins that you can use to incorporate into workflows such technologies as the VMware vCenter Server API and email capabilities. In addition, you can use the Orchestrator open plug-in architecture to develop plug-ins to access other applications.

The Orchestrator plug-ins that VMware develops are distributed as .vmoapp files, which you can obtain from the VMware Web site at http://www.vmware.com/products/datacenter-virtualization/vcenter-orchestrator/plugins.html. For more information about the Orchestrator plug-ins that VMware develops and distributes, see http://www.vmware.com/support/pubs/vco_plugins_pubs.html.
Overview of the Orchestrator Appliance

The Orchestrator Appliance is a preconfigured Linux-based virtual machine optimized for running vCenter Orchestrator.

The Orchestrator Appliance package contains the following software:

- SUSE Linux Enterprise Server 11 Update 1 for VMware, 64-bit edition
- PostgreSQL
- OpenLDAP
- Orchestrator 5.1

The default Orchestrator Appliance database configuration is suitable for small- or medium-scale environment. The default OpenLDAP configuration is suitable for experimental and testing purposes only. To use the Orchestrator Appliance in a production environment, set up a new database and directory service, and configure the Orchestrator server to work with them. You can also configure the Orchestrator server to work with VMware vCenter Single Sign On. For more information about configuring external LDAP or vCenter Single Sign On, and database for production environments, see “Selecting the Authentication Type,” on page 26 and “Orchestrator Database Setup,” on page 34.

The Orchestrator Appliance has the following hardware configuration:

- 2 CPUs
- 3GB of memory
- 7GB hard disk

Do not reduce the default memory size, because the Orchestrator server requires at least 2GB of free memory.

The configuration maximums for the Orchestrator Appliance are the same as the maximums for vCenter Orchestrator. For more information, see Configuration Maximums at http://www.vmware.com/pdf/vsphere5/r50/vsphere-50-configuration-maximums.pdf.

This chapter includes the following topics:

- “Download and Deploy the Orchestrator Appliance,” on page 12
- “Power On the Orchestrator Appliance and Log In to the Appliance Web Console,” on page 13
Download and Deploy the Orchestrator Appliance

As an alternative to installing vCenter Orchestrator on a Windows computer, you can download and deploy the Orchestrator Appliance.

The steps in the procedure might vary depending on the version of the vSphere Client that you use. You can also deploy the Orchestrator Appliance by using the vSphere Web Client. For instructions, see vSphere Virtual Machine Administration.

Prerequisites

Verify that your computing environment meets the following conditions:

- vCenter Server is installed and running.
- vSphere Client is installed.
- The host on which you are deploying the appliance has enough free disk space.

In case that your system is isolated and without Internet access, you must download the .vmdk and .ovf files for the appliance from the download page on the VMware Web site, and save the files in the same folder.

Procedure

1. Log in to the vSphere Client as an administrator.
2. In the vSphere Client, select File > Deploy OVF Template.
3. Enter the path or the URL to the .ovf file and click Next.
4. Review the OVF details and click Next.
5. Accept the terms in the license agreement and click Next.
6. Specify a name and location for the deployed appliance and select a host or cluster on which to run the appliance.
7. Select a format in which to store the appliance’s virtual disk.

<table>
<thead>
<tr>
<th>Format</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Thick provisioned Lazy Zeroed</td>
<td>Creates a virtual disk in a default thick format. Space required for the virtual disk is allocated when the virtual disk is created. Data remaining on the physical device is not erased during creation, but is zeroed out on demand at a later time on first write from the virtual machine.</td>
</tr>
<tr>
<td>Thick Provisioned Eager Zeroed</td>
<td>Supports clustering features such as Fault Tolerance. Space required for the virtual disk is allocated at creation time. In contrast to the flat format, the data remaining on the physical device is zeroed out when the virtual disk is created. It might take much longer to create disks in this format than to create other types of disk formats.</td>
</tr>
<tr>
<td>Thin provisioned format</td>
<td>Saves storage space. For the thin disk, you provision as much datastore space as the disk would require based on the value that you enter for the disk size. However, the thin disk starts small and at first, uses only as much datastore space as the disk needs for its initial operations.</td>
</tr>
</tbody>
</table>

8. (Optional) Specify the network settings and IP address allocation, and click Next.

By default the Orchestrator Appliance uses DHCP. You can also change this setting manually and assign a fixed IP address from the appliance Web console.

9. Review the properties and the Ready to Complete Page and optionally select to power on the appliance after deployment.

10. Click Finish.
The Orchestrator Appliance is successfully deployed.

**Power On the Orchestrator Appliance and Log In to the Appliance Web Console**

To use the Orchestrator Appliance, you must first power it on and get the virtual appliance IP address.

**Procedure**

1. Log in to the vSphere Client as an administrator.
2. Right-click the Orchestrator Appliance and select **Power > Power On**.
3. Click the **Summary** tab to view the Orchestrator Appliance IP address.
4. In a Web browser, navigate to the IP address that your Orchestrator Appliance virtual machine provides.
   
   http://orchestrator_appliance_ip

5. Click **Appliance Configuration**.

6. Type the default appliance user name and password.
   - User name: **root**.
   - Password: **vmware**.
Configuring the Orchestrator Appliance

The Orchestrator Appliance is a preconfigured Linux-based virtual appliance. Before you use it, you might want to edit some of the configuration settings of the appliance.

The Orchestrator Appliance is built with VMware Studio. For more information about virtual appliances created with VMware Studio, see the VMware Studio documentation at http://www.vmware.com/support/developer/studio/index.html.

This chapter includes the following topics:
- “Log In to the Orchestrator Appliance Web Console,” on page 15
- “Change the Default Root Password,” on page 16
- “Enable or Disable SSH Administrator Login on the vCenter Orchestrator Appliance,” on page 16
- “Configure Network Settings for the Orchestrator Appliance,” on page 16
- “Upgrading the Orchestrator Appliance,” on page 17

Log In to the Orchestrator Appliance Web Console

Log in to the Orchestrator Appliance Web console to access the appliance configuration settings.

Prerequisites
- Download and deploy the Orchestrator Appliance.
- Ensure that the appliance is up and running.

Procedure
1. In a Web browser, navigate to the IP address that your Orchestrator Appliance virtual machine provides.
   http://orchestrator_appliance_ip
2. Click Appliance Configuration to go to the appliance Web console.
3. Type the Orchestrator Appliance user name and password, and click Login.

You can view the system settings of the Orchestrator Appliance, such as vendor, appliance name, and version.

What to do next
Edit the network or update settings of the appliance.
Change the Default Root Password

For security reasons, you must change the root password of the Orchestrator Appliance.

**Prerequisites**
- Download and deploy the Orchestrator Appliance.
- Ensure that the appliance is up and running.

**Procedure**
1. Log in to the appliance Web console.
2. Click the **Admin** tab.
3. In the **Current administrator password** text box type the current root password.
4. Type the new password in the **New administrator password** and **Retype new administrator password** text boxes.
5. Click **Change password**.

You successfully changed the password of the root Linux user of the Orchestrator Appliance.

Enable or Disable SSH Administrator Login on the vCenter Orchestrator Appliance

You can enable or disable the ability to log in as root to the Orchestrator Appliance using SSH.

**Prerequisites**
- Download and deploy the Orchestrator Appliance.
- Ensure that the appliance is up and running.

**Procedure**
1. Log in to the Orchestrator Appliance Web console.
2. On the **Admin** tab, click **Toggle SSH setting** to allow log in as root to the Orchestrator Appliance using SSH.
3. (Optional) Click **Toggle SSH setting** again to prevent log in as root to the Orchestrator Appliance using SSH.

Configure Network Settings for the Orchestrator Appliance

Configure network settings for the Orchestrator Appliance to assign a static IP and define the proxy settings.

**Prerequisites**
- Download and deploy the Orchestrator Appliance.
- Ensure that the appliance is up and running.

**Procedure**
1. Log in to the Orchestrator Appliance Web console.
2. On the **Network** tab, click **Address**.
3 Select the method by which the appliance obtains IP address settings.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHCP</td>
<td>Obtains IP settings from a DHCP server. This is the default setting.</td>
</tr>
<tr>
<td>Static</td>
<td>Uses static IP settings. Specify the IP address, netmask, and gateway.</td>
</tr>
</tbody>
</table>

4 (Optional) Type the necessary network configuration information.

5 Click **Save Settings**.

6 (Optional) Use a proxy server for the Orchestrator Appliance.
   a On the **Network** tab, click **Proxy**.
   b Select **Use a proxy server** to use a proxy server for the Orchestrator Appliance.
   c Specify a proxy server and a proxy port.
   d Type a proxy user name and proxy password if your proxy server requires them.
   e Click **Save Settings**.

### Upgrading the Orchestrator Appliance

You can upgrade the deployed Orchestrator Appliance with packages that VMware publishes. You can perform updates over the external Web, on your local area network, or from a CD-ROM.

To conserve network bandwidth, virtual appliance updates are applied only to packages that have changed. Updates can apply to the operating system, applications in the virtual appliance, VMware Tools, or the VMware Appliance Management Infrastructure (VAMI).

If you have installed VMware vSphere® Update Manager you can use it to update the Orchestrator Appliance automatically. For more information about upgrading virtual appliances with vSphere Update Manager, see the Update Manager documentation at [http://www.vmware.com/support/pubs/vum_pubs.html](http://www.vmware.com/support/pubs/vum_pubs.html).

After you upgrade the Orchestrator Appliance your plug-ins’ settings are preserved. If you want to configure the Orchestrator server to work with vCenter Single Sign On you must provide the vCenter Single Sign On credentials on the **Plug-ins** tab of the Orchestrator configuration interface.

### Check the Orchestrator Appliance Version Status

You might want to see and check the Orchestrator Appliance version status before you configure the appliance for updates.

**Prerequisites**
- Download and deploy the Orchestrator Appliance.
- Ensure that the appliance is up and running.

**Procedure**
1 Log in to the Orchestrator Appliance Web console.
2 On the **Update** tab, click **Status**.

You see the update status of the Orchestrator Appliance.

**What to do next**
Configure the Orchestrator Appliance for updates.
Configure the Orchestrator Appliance for Updates

You can update a deployed Orchestrator Appliance with packages that VMware publishes. You can perform updates over the external Web, on your local area network, or from a CD-ROM.

Prerequisites

- Download and deploy the Orchestrator Appliance.
- Ensure that the appliance is up and running.

Procedure

1. Log in to the Orchestrator Appliance Web console.
2. On the Update tab, click Settings.
3. Set an update policy for the virtual appliance.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>No automatic updates</td>
<td>The virtual appliance does not check for and install updates.</td>
</tr>
<tr>
<td>Automatic check for updates</td>
<td>The virtual appliance checks for updates at the scheduled time. If an update is available, it appears on the Update Status page.</td>
</tr>
<tr>
<td>Automatic check and install updates</td>
<td>The virtual appliance checks for updates at the scheduled time. If an update is available, the virtual appliance installs it.</td>
</tr>
</tbody>
</table>

If you select either Automatic check for updates or Automatic check and install updates, you can configure the scheduling. By default, the check occurs daily at 03:00 local time, as determined by your time zone settings.

4. Set up the update repository location.

The default is the URL that VMware configured. You might need to change the update source or location if you are updating inside a restricted local area network.

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use CD-ROM Updates</td>
<td>Insert the update CD-ROM in a drive that the virtual appliance can read. The update agent scans the CD drives to find the first update CD-ROM.</td>
</tr>
<tr>
<td>Use Specified Repository</td>
<td>Type the URL of the update repository for your appliance to check. If the URL requires authentication, provide a valid user name and password.</td>
</tr>
</tbody>
</table>

5. Click Save Settings.

Install Available Updates Manually

When new updates for the Orchestrator Appliance become available, you might want to install them to keep your appliance up-to-date.

Prerequisites

- Download and deploy the Orchestrator Appliance.
- Ensure that the appliance is up and running.

Procedure

1. Log in to the Orchestrator Appliance Web console.
2. On the Update tab, click Status.
3 Under the Actions section, click **Check Updates**.

The virtual appliance connects to the update repository and checks for available updates. Updates appear in the **Available Updates** pane.

4 To install an update, click **Install Updates**.
Although the Orchestrator Appliance is a preconfigured Linux-based virtual machine, you must install and configure the default vCenter Server plug-in as well as the other default Orchestrator plug-ins. In addition, you might also want to change the Orchestrator settings.

For instructions about installing and configuring the default Mail and SSH plug-ins, see Installing and Configuring VMware vCenter Orchestrator.

If you want to use the Orchestrator Appliance in a medium or large-scale environment, you might want to also change the LDAP and database settings.

The Orchestrator Appliance contains a preconfigured PostgreSQL database and OpenLDAP server. The PostgreSQL database and OpenLDAP server are accessible only locally from the virtual appliance Linux console.

<table>
<thead>
<tr>
<th>Preconfigured Software</th>
<th>User Group (if any) and User</th>
<th>Password</th>
</tr>
</thead>
<tbody>
<tr>
<td>PostgreSQL</td>
<td>User: vmware</td>
<td>vmware</td>
</tr>
<tr>
<td>OpenLDAP</td>
<td>User group: vcoadmins</td>
<td>vcoadmin</td>
</tr>
<tr>
<td></td>
<td>User: vcoadmin</td>
<td></td>
</tr>
<tr>
<td></td>
<td>By default the vcoadmin user is set up as an Orchestrator administrator.</td>
<td></td>
</tr>
<tr>
<td>OpenLDAP</td>
<td>User group: vcousers</td>
<td>vcouser</td>
</tr>
<tr>
<td></td>
<td>User: vcouser</td>
<td></td>
</tr>
</tbody>
</table>

PostgreSQL and OpenLDAP are suitable for small- to medium-scale production environments. To use the Orchestrator appliance in a large-scale production environment, you should replace PostgreSQL with an external database instance and OpenLDAP with an external supported directory service or with VMware vCenter Single Sign On. For more information about setting up an external database, see “Configure the Database Connection,” on page 36. For information about setting up an external directory service or vCenter Single Sign On, see “Selecting the Authentication Type,” on page 26.

You can additionally configure the Orchestrator server to work with vCenter Single Sign On prebuilt in the vCenter Server Appliance. For more information about configuring the Orchestrator server and registering Orchestrator with vCenter Single Sign On prebuilt in the vCenter Server Appliance, see Installing and Configuring VMware vCenter Orchestrator.

This chapter includes the following topics:

- “Log In to the Orchestrator Configuration Interface,” on page 22
- “Import a vCenter Server SSL Certificate and License,” on page 22
- “Install and Configure the vCenter Server Plug-In,” on page 23
- “Selecting the Authentication Type,” on page 26
- “Orchestrator Database Setup,” on page 34
Log In to the Orchestrator Configuration Interface

To edit the default configuration settings of the Orchestrator server and to assign a server certificate, you must log in to the Orchestrator configuration interface.

Prerequisites

- Download and deploy the Orchestrator Appliance.
- Ensure that the appliance is up and running.

Procedure

1. In a Web browser, navigate to the IP address that your Orchestrator Appliance virtual machine provides.
   http://orchestrator_appliance_ip
2. Click Orchestrator Configuration.
3. Log in with the default credentials.
   - User name: vmware
     You cannot change the default user name.
   - Password: vmware
     When you log in to the Orchestrator configuration interface with the default password, you see the Welcome page prompting you to change the default password of the Orchestrator configuration interface.
4. Type and confirm your new password.
5. Click Apply changes.

Import a vCenter Server SSL Certificate and License

The Orchestrator Appliance is distributed with a built-in evaluation license that expires 90 days after you power on the appliance for the first time. To continue using the Orchestrator Appliance after the trial period, you must import a vCenter Server license.

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.

For more information about vCenter Server license and access rights to the Orchestrator server, see Installing and Configuring VMware vCenter Orchestrator.

Procedure

1. Log in to the Orchestrator configuration interface as vmware.
2. Click Network.
3. In the right pane, click the SSL Certificate tab.
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>Import from URL</td>
<td>Type the URL of the vCenter Server system:</td>
</tr>
<tr>
<td></td>
<td><code>https://your_vcenter_server_IP_address</code> or</td>
</tr>
<tr>
<td></td>
<td><code>your_vcenter_server_IP_address:port</code></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Import from file</th>
<th>Obtain the vCenter Server certificate file. The file is usually available at the following locations:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>- <code>C:\Documents and Settings\AllUsers\ApplicationData\VMware\VMware VirtualCenter\SSL\rui.crt</code></td>
</tr>
<tr>
<td></td>
<td>- <code>/etc/vmware/ssl/rui.crt</code></td>
</tr>
</tbody>
</table>

5. Click **Import**.

A message confirming that the import is successful appears.

6. In the Orchestrator configuration interface, click **Licenses**.

7. Click the **vCenter Server License** tab, and click **Use vCenter Server license**.

8. Specify the details about the vCenter Server machine on which Orchestrator must verify the license key.

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host</td>
<td>Type the IP address or the DNS name of the vCenter Server system.</td>
</tr>
<tr>
<td>Port</td>
<td>Leave the default value (443).</td>
</tr>
<tr>
<td>Secure channel</td>
<td>(Optional) Select to establish a secure connection to the vCenter Server system.</td>
</tr>
<tr>
<td>Path</td>
<td>Use the default value, <code>/sdk</code>.</td>
</tr>
<tr>
<td>User name</td>
<td>Type the credentials that Orchestrator must use to establish the connection to vCenter Server. The user you select must be a valid user with administrative privileges on your vCenter Server system, preferably at the top of the vSphere tree structure.</td>
</tr>
<tr>
<td>Password</td>
<td>Type the credentials that Orchestrator must use to establish the connection to vCenter Server.</td>
</tr>
</tbody>
</table>

9. Click **Apply changes**.

10. Restart the Orchestrator server.

**Install and Configure the vCenter Server Plug-In**

Orchestrator uses the vCenter Web Service API to control vCenter Server. You can install the vCenter Server plug-in and then set the parameters to enable Orchestrator to connect to your vCenter Sever instances.

**Procedure**

1. **Install the vCenter Server Plug-In** on page 24

To run workflows over the objects in your vCenter Server inventory, you must install and configure the vCenter Server plug-in. You must install the vCenter Server plug-in before configuring it.

2. **Import the vCenter Server SSL Certificate** on page 24

The Orchestrator configuration interface uses a secure connection to communicate with vCenter Server, relational database management system (RDBMS), LDAP, vCenter Single Sign On, or other servers. You can import the required SSL certificate from a URL or file.
You can configure Orchestrator to connect to your vCenter Server instances to run workflows over the objects in your vSphere infrastructure.

**Install the vCenter Server Plug-In**

To run workflows over the objects in your vCenter Server inventory, you must install and configure the vCenter Server plug-in. You must install the vCenter Server plug-in before configuring it.

**Procedure**

1. Log in to the Orchestrator configuration interface as `vmware`.
2. Click the **Plug-ins** tab.
3. (Optional) Provide the credentials of a user who is a member of the Orchestrator Admin group.
   By default, the credentials of the vcoadmin user of the OpenLDAP server are provided.
4. In the list of plug-ins on the right, select **vCenter Server**, and click **Apply changes**.
5. On the **Startup options** tab, click **Restart the vCO configuration server**.
   The **vCenter Server** plug-in tab becomes active and you can configure the connection between vCenter Orchestrator and vCenter Server instances.

**Import the vCenter Server SSL Certificate**

The Orchestrator configuration interface uses a secure connection to communicate with vCenter Server, relational database management system (RDBMS), LDAP, vCenter Single Sign On, or other servers. You can import the required SSL certificate from a URL or file.

You can import the vCenter Server SSL certificate from the **SSL Trust Manager** tab in the Orchestrator configuration interface.

**Procedure**

1. Log in to the Orchestrator configuration interface as `vmware`.
2. Click **Network**.
3. In the right pane, click the **SSL Trust Manager** 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>
</table>
| **Import from URL** | Specify the URL of the vCenter Server:  
  https://your_vcenter_server_IP_address or  
  your_vcenter_server_IP_address:port |
| **Import from file** | Obtain the vCenter Server certificate file. The file is usually available at the following locations:  
  - C:\Documents and Settings\AllUsers\ApplicationData\VMware\VirtualCenter\SSL\rui.crt  
  - /etc/vmware/ssl/rui.crt |

5. Click **Import**.
   A message confirming that the import is successful appears.
6. Repeat the steps for each vCenter Server 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 SSL Trust Manager on the Network tab and import the corresponding vCenter Server SSL certificate.

**Configure the vCenter Server 5.1 Plug-In**

You can configure Orchestrator to connect to your vCenter Server instances to run workflows over the objects in your vSphere infrastructure.

To manage the objects in your vSphere inventory by using the vSphere Web Client, make sure that you configure the Orchestrator server to work with the vCenter Server instance registered with the vSphere Web Client that uses the same vCenter Single Sign On instance with which you registered Orchestrator.

**Prerequisites**

Import the SSL certificates for each vCenter Server instance you define.

**Procedure**

1. Log in to the Orchestrator configuration interface as `vmware`.
2. Click vCenter Server, and click the New vCenter Server Host tab.
3. From the Available drop-down menu, select Enabled.
4. In the Host text box, type the IP address or the DNS name of the machine on which the vCenter Server instance you want to add is installed.
5. In the Port text box, retain the default value, 443.
6. (Optional) Select the Secure channel check box to establish a secure connection to your vCenter Server machine.
7. In the Path text box, retain the default value, `/sdk`.

This value is the location of the SDK that you use to connect to your vCenter Server instance.
8 Select the method you want to use to manage user access on the vCenter Server system.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Share a unique session</td>
<td>Allows Orchestrator to create only one connection to vCenter Server. In the <strong>User name</strong> and <strong>Password</strong> 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 privileges to manage vCenter Server extensions and a set of custom defined privileges. Orchestrator uses these credentials to monitor the vCenter Web service, typically to operate Orchestrator system workflows.</td>
</tr>
<tr>
<td>Session per user</td>
<td>Creates a new session to vCenter Server. This might rapidly use CPU, memory, and bandwidth. Select this option only if your vCenter Server is in an Active Directory domain or if vCenter Server Sign On is enabled. The user that you select must be a valid user with privileges to manage vCenter Server extensions. You can leave the <strong>User name</strong> and <strong>Password</strong> text boxes empty, because the credentials are used only for connection check.</td>
</tr>
</tbody>
</table>

The user account that you select is also used by the policy engine to collect statistical and other data. If the user that you select does not have enough privileges, the policy engine cannot access the necessary parts of the vCenter Server inventory and thus cannot collect the necessary data.

9 Click **Apply changes**.

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

10 Repeat Step 2 through Step 9 for each vCenter Server instance.

**Selecting the Authentication Type**

The Orchestrator Appliance contains a preconfigured OpenLDAP server that is suitable for experimental use in small- and medium-scale environments. To use the Orchestrator Appliance in a large-scale environment for production purposes, you can either set up a new directory service server and configure Orchestrator to work with it or configure Orchestrator to work with vCenter Single Sign On.

Orchestrator 5.1 supports two types of authentications:

- **LDAP authentication** — Orchestrator connects to a working LDAP server.
- **vCenter Single Sign On authentication** — Orchestrator authenticates through vCenter Single Sign On.

**IMPORTANT** If you want to use vCenter Orchestrator through the vSphere Web Client for managing vSphere inventory objects, you must configure Orchestrator to authenticate through vCenter Single Sign On.

**Configuring vCenter Single Sign On Settings**

VMware vCenter Single Sign On is an authentication service that implements the brokered authentication architectural pattern. You can configure Orchestrator to connect to a vCenter Single Sign On server.

The vCenter Single Sign On server provides an authentication interface called Security Token Service (STS). Clients send authentication messages to the STS, which checks the user’s credentials against one of the identity sources. Upon successful authentication, STS generates a token.

In vCenter Server versions earlier than vCenter Server 5.1, when a user connects to vCenter Server, vCenter Server authenticates the user by validating the user against an Active Directory domain or the list of local operating system users. In vCenter Server 5.1, users authenticate through vCenter Single Sign On.
The vCenter Single Sign On administrative interface is part of the vSphere Web Client. To configure vCenter Single Sign On and manage vCenter Single Sign On users and groups, you log in to the vSphere Web Client as a user with vCenter Single Sign On administrator privileges. This might not be the same user as the vCenter Server administrator. Enter the credentials on the vSphere Web Client login page and upon authentication, you can access the vCenter Single Sign On administration tool to create users and assign administrative permissions to other users.

Using the vSphere Web Client, you authenticate to vCenter Single Sign On by entering your credentials on the vSphere Web Client login page. You can then view all of the vCenter Server instances for which you have permissions. After you connect to vCenter Server, no further authentication is required. The actions that you can perform on objects depend on the user's vCenter Server permissions on those objects.

For more information about vCenter Single Sign On, see vSphere Security.

After you configure Orchestrator to authenticate through vCenter Single Sign On, make sure that you configure it to work with the vCenter Server instances registered with the vSphere Web Client using the same vCenter Single Sign On instance.

When you log in to the vSphere Web Client, the Orchestrator Web plug-in communicates with the Orchestrator server on behalf of the user profile you used to log in.

**Import the vCenter Single Sign On SSL Certificate**

To register Orchestrator as a vCenter Single Sign On solution and configure it to work with vCenter Single Sign On, first import the vCenter Single Sign On SSL certificate.

You can import the vCenter Single Sign On SSL certificate from the SSL Trust Manager tab in the Orchestrator configuration interface.

**Prerequisites**

Install and configure vCenter Single Sign On.

**Procedure**

1. Log in to the Orchestrator configuration interface as **vmware**.
2. Click **Network**.
3. In the right pane, click the **SSL Trust Manager** tab.
4. Load the vCenter Single Sign On SSL certificate from a URL or a file.

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
</table>
| **Import from URL** | Type the URL of the vCenter Single Sign On server:  
https://your_vcenter_single_sign_on_server_IP_address:7444  
or  your_vcenter_single_sign_on_server_IP_address:7444 |
| **Import from file** | Obtain the vCenter Single Sign On SSL certificate file and browse to import it. |

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.

You successfully imported the vCenter Single Sign On certificate.
What to do next

Register Orchestrator as an vCenter Single Sign On extension and configure additional vCenter Single Sign On settings.

Register Orchestrator as a vCenter Single Sign On Solution in Basic Mode

You can register the Orchestrator server with a vCenter Single Sign On server by using the simple mode registration form in the Orchestrator configuration interface. The simple mode registration is easier and initially you should only provide the URL of your vCenter Single Sign On server and the credentials of the vCenter Single Sign On admin.

Prerequisites

Install and configure VMware vCenter Single Sign On and verify that your vCenter Single Sign On server is running.

Procedure

1. Log in to the Orchestrator configuration interface as **vmware**.
2. Click **Authentication**.
3. Select **SSO Authentication** from the **Authentication mode** drop-down menu.
4. In the **Host** text box, type the URL for the machine on which you have installed the vCenter Single Sign On server.
   
   https://your_vcenter_single_sign_on_server:7444

5. In the **Admin user name** and **Admin password** text boxes, type the credentials of the vCenter Single Sign On admin.

   The account is temporarily used only for registering or removing Orchestrator as a solution.

6. Click **Register Orchestrator**.
7. Complete the vCenter Single Sign On configuration.
   a. (Optional) Filter the list of available groups by typing search criteria in the **Groups filter** text box and pressing Enter.
   b. Select a vCO Admin domain and group from the drop-down menu.
   c. (Optional) Modify the value for the time difference between a client clock and a domain controller clock.

   The default clock tolerance value is 300 seconds.

8. Click **Accept Orchestrator Configuration**.

You successfully registered Orchestrator with vCenter Single Sign On.

Register Orchestrator as a vCenter Single Sign On Solution in Advanced Mode

You can register the Orchestrator server with a vCenter Single Sign On server by using the advanced mode registration form in the Orchestrator configuration interface. In the advanced mode you manually type the token service URL, the administration service URL, and they are not automatically generated for you.

Prerequisites

Install and configure vCenter Single Sign On and verify that your vCenter Single Sign On server is running.

Procedure

1. Log in to the Orchestrator configuration interface as **vmware**.
2 Click **Authentication**.
3 Select **SSO Authentication** from the **Authentication mode** drop-down menu.
4 Click the **Advanced settings** link.
5 In the **Token service URL** text box, type the URL for the vCenter Single Sign On token service interface.
   https://your_vcenter_single_sign_on_server:7444/ims/STSService
6 In the **Admin service URL** text box, type the URL for the vCenter Single Sign On administration service interface.
   https://your_vcenter_single_sign_on_server:7444/sso-adminserver/sdk
7 In the **Admin user name** and **Admin password** text boxes, type the credentials of the vCenter Single Sign On admin.
   The account is temporarily used only for registering or removing Orchestrator as a solution.
8 Click **Register Orchestrator**.
9 Complete the vCenter Single Sign On configuration.
   a (Optional) Filter the list of available groups by typing search criteria in the **Groups filter** text box and pressing Enter.
   b Select a vCO Admin domain and group from the drop-down menu.
   c (Optional) Modify the value for the time difference between a client clock and a domain controller clock.
      The default clock tolerance value is 300 seconds.
10 Click **Accept Orchestrator Configuration**.
   You successfully registered Orchestrator with vCenter Single Sign On.

**Configuring LDAP Settings**

The Orchestrator Appliance contains a preconfigured OpenLDAP server that is suitable for experimental use in small- and medium-scale environments. To use the Orchestrator Appliance in a large-scale environment for production purposes, you can set up a new directory service server and configure Orchestrator to work with it.


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 small 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.

**IMPORTANT** Multiple domains that are not in the same tree, but have a two-way trust, are not supported and do not work with Orchestrator. The only configuration supported for multi-domain Active Directory is domain tree. Forest and external trusts are not supported.
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.

You can import the LDAP SSL certificate from the SSL Trust Manager tab in the Orchestrator configuration interface.

Prerequisites

- If you are using LDAP servers, 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.
- Configure your LDAP server for SSL access. See the documentation of your LDAP server for instructions.
- Explicitly specify the trusted certificate to perform the SSL authorization correctly.

Procedure

1. Log in to the Orchestrator configuration interface as **vmware**.
2. Click **Network**.
3. In the right pane, click the **SSL Trust Manager** tab.
4. Browse to select a certificate file to import.
5. Load the LDAP SSL certificate from a URL or a file.

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Import from URL</strong></td>
<td>Type the URL of the LDAP server:</td>
</tr>
<tr>
<td></td>
<td><strong>https://your_LDAP_server_IP_address</strong> or</td>
</tr>
<tr>
<td></td>
<td><strong>your_LDAP_server_IP_address:port</strong></td>
</tr>
<tr>
<td><strong>Import from file</strong></td>
<td>Obtain the LDAP SSL certificate file and browse to import it.</td>
</tr>
</tbody>
</table>

6. Click **Import**.
   A message confirming that the import is successful appears.
7. Click **Startup Options**.
8. Click **Restart the vCO configuration server** to restart the Orchestrator Configuration service after adding a new SSL certificate.

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

What to do next

When you generate the LDAP connection URL you should enable SSL on the **Authentication** tab in the Orchestrator configuration interface.

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 **Authentication**.
3. Select **LDAP Authentication** from the **Authentication mode** drop-down menu.
4. 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.

5. In the **Primary LDAP host** text box, type the IP address or the DNS name of the host on which your primary LDAP service runs.
   
   This is the first host on which the Orchestrator configuration interface verifies user credentials.

6. (Optional) In the **Secondary LDAP host** text box, type the IP address or the DNS name of the host on which your secondary LDAP service runs.
   
   If the primary LDAP host becomes unavailable, Orchestrator verifies user credentials on the secondary host.

7. In the **Port** text box, type the value for the 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.

8. In the **Root** text box, type the root element of your LDAP service.
   
   If your domain name is **company.org**, your root LDAP is **dc=company,dc=org**.
   
   This is the node used 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.

9. (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 30.

10. (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 32.

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 Authentication.
3. Select LDAP Authentication from the Authentication mode drop-down menu.
4. Specify the primary and secondary LDAP hosts, the lookup port of the LDAP server, and the root element.
5. 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.
6. In the Password text box, type the password for the user name you entered in Step 5.

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 Authentication.
3. Select LDAP Authentication from the Authentication mode drop-down menu.
4. Specify the primary and secondary LDAP hosts, the lookup port of the LDAP server, the root element, and the browsing credentials.
5. 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.

6. 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.

7. 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.

8. 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, type 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 un Java System Directory Server, you must select the Dereference links check box.
5. (Optional) Select the Filter attributes check box to filter the attributes that the search returns.
   Selecting this check box makes searching in LDAP faster. 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, type a value in milliseconds.
   This value determines the timeout period for the test that is 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.

Orchestrator Database Setup

The Orchestrator Appliance contains a preconfigured and prepopulated PostgreSQL database that is suitable for small- and medium-scale environments. To use the Orchestrator Appliance in a production environment, set up a new database and configure the Orchestrator server to connect to that database.

In addition, the Orchestrator server supports Microsoft SQL Server, Oracle, and MySQL databases.

The common workflow for setting up the Orchestrator database involves the following tasks:

1. Install a relational database management system (RDBMS), and create a new database. For more information about creating a new database, see the documentation of your Microsoft or Oracle database provider.
2. Enable the database for remote connection.
3. Configure the database connection parameters. For more information, see “Configure the Database Connection,” on page 36.

The way in which your database is set up can affect Orchestrator performance.
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 located. Insufficient disk storage space might result in unwanted behavior of the Orchestrator server and client.

**Import the Database SSL Certificate**

If your database uses SSL, you must import the SSL certificate to the Orchestrator configuration interface and activate secure connection between Orchestrator and the database.

You can import the database SSL certificate from the **SSL Trust Manager** tab in the Orchestrator configuration interface.

**Prerequisites**

- Configure your database for SSL access. See your database documentation for instructions.
- Obtain a self-signed server certificate or a certificate that is signed by a Certificate Authority.
- Explicitly specify the trusted certificate to perform the SSL authorization correctly.

**Procedure**

1. Log in to the Orchestrator configuration interface as **vmware**.
2. Click **Network**.
3. In the right pane, click the **SSL Trust Manager** tab.
4. Load the database SSL certificate from a URL or a file.

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Import from URL</td>
<td>Type the URL of the database server:</td>
</tr>
<tr>
<td></td>
<td>https://your_database_server_IP_address</td>
</tr>
<tr>
<td></td>
<td>or</td>
</tr>
<tr>
<td></td>
<td>your_database_server_IP_address:port</td>
</tr>
</tbody>
</table>

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 Certificates list. The secure connection between Orchestrator and your database is activated.

**What to do next**

When you configure the database connection you should enable SSL on the **Database** tab in the Orchestrator configuration interface.
Configure the Database Connection

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

Prerequisites

- 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 you configure the database connection and build the table structure for Orchestrator. This setting is crucial for an internationalized environment.
- To configure Orchestrator to communicate with the database over a secure connection, make sure that you import the database SSL certificate. For more information, see “Import the Database SSL Certificate,” on page 35.

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 that you want Orchestrator server to use.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oracle</td>
<td>Configures Orchestrator to work with an Oracle database instance.</td>
</tr>
<tr>
<td>SQL Server</td>
<td>Configures Orchestrator to work with a Microsoft SQL Server or Microsoft SQL Server Express database instance.</td>
</tr>
<tr>
<td>MySQL</td>
<td>Configures Orchestrator to work with a MySQL database instance.</td>
</tr>
<tr>
<td>PostgreSQL</td>
<td>Configures Orchestrator to work with a PostgreSQL database instance.</td>
</tr>
</tbody>
</table>

4. Define the database connection parameters and click Apply changes.

<table>
<thead>
<tr>
<th>Option</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 db_owner rights. This option is applicable for all databases.</td>
</tr>
<tr>
<td>Password (if any)</td>
<td>The password for the user name. This option is applicable for all databases.</td>
</tr>
<tr>
<td>Use SSL</td>
<td>Specifies whether you want to use SSL connection to the database. To use this option you must make sure that you import the database SSL certificate into Orchestrator. This option is applicable for all databases.</td>
</tr>
<tr>
<td>Database server IP address or DNS name</td>
<td>The database server IP address or DNS name. This option is applicable for all databases.</td>
</tr>
<tr>
<td>Port</td>
<td>The full unique name of your database. The database name is specified by the SERVICE_NAMES parameter in the initialization parameter file. This option is valid only for SQL Server, MySQL, and PostgreSQL databases.</td>
</tr>
<tr>
<td>Database name</td>
<td>The name of the database instance that can be identified by the INSTANCE_NAME parameter in the database initialization parameter file. This option is valid only for SQL Server and Oracle databases.</td>
</tr>
<tr>
<td>Instance name (if any)</td>
<td>The name of the database instance that can be identified by the INSTANCE_NAME parameter in the database initialization parameter file. This option is valid only for SQL Server and Oracle databases.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Domain</strong></td>
<td>To use Windows authentication, type the domain name of the SQL Server machine, for example <code>company.org</code>. To use SQL authentication, leave this text box blank.</td>
</tr>
<tr>
<td><strong>Use Windows authentication mode (NTLMv2)</strong></td>
<td>Select to send NTLMv2 responses when using Windows authentication. This option is valid only for SQL Server.</td>
</tr>
</tbody>
</table>

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 build or update the database table structure.

5. (Optional) Build or update the table structure for Orchestrator.

<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 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**.

The database connection is successfully configured.

**Changing SSL Certificates**

By default, the Orchestrator server and Orchestrator configuration server use a self-signed SSL certificate to communicate remotely with the Orchestrator client. Orchestrator also provides an SSL certificate that controls user access to Web views.

The Orchestrator Appliance uses light-httpd to run its own management site.

You can change the SSL certificates, for example if your company security policy requires you to use its SSL certificates.

**Generate a New Certificate**

To change an SSL certificate, you can generate a new keystore file. You can generate the new keystore in the Orchestrator Appliance machine.

**Prerequisites**

To generate the new certificate, you must use the Java `keytool` utility. You can find the utility in the system Orchestrator Appliance virtual machine.

**Procedure**

1. Log in to the appliance Linux console as root and navigate to the `keytool` utility.

   The default location is:

   `/opt/vmo/jre/bin/keytool`
2 Create a local certificate.

```
keytool -genkey -alias mySslCertificate -keyalg RSA -keystore <your_keystore_filename> \
-keysize 2048 -sigalg SHA512withRSA
```

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

What to do next

You can create a signing request and submit the certificate to a Certificate Authority. You can then import the signed certificate into your local keystore.

You can also change the Web views SSL certificate, the SSL certificate for the Orchestrator configuration interface, or the SSL certificate for the Orchestrator client with the certificate you generated.

Install a Certificate from a Certificate Authority

To install a certificate signed from a Certificate Authority you must obtain an SSL certificate from a CA and import it in your local keystore.

Prerequisites

Make sure that you have generated a new SSL certificate.

Procedure

1 (Optional) Create a certificate signing request by running the following command in the Java utility.

```
keytool -certreq -alias mySslCertificate -file certreq.csr \
-keystore <your_keystore_filename>
```

The utility generates a file called `certreq.csr`.

2 (Optional) Submit the `certreq.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. The CA returns a certificate that you must import.

3 (Optional) Import the SSL certificate in your local keystore.

   a Download a root certificate from the CA that signed your certificate.

   b Import the root certificate in your keystore by running following command in the Java utility.

   ```
   keytool -import -alias root -keystore <your_keystore_filename> \
   -trustcacerts -file <filename_of_the_root_certificate>
   ```

   c Import the SSL certificate signed by the CA (the SSL certificate must be in X509 format).

   ```
   keytool -import -alias mySslCertificate -keystore <your_keystore_filename> \
   -trustcacerts -file <your_certificate_filename>
   ```

The SSL certificate is installed. You can change the Web views SSL certificate, the SSL certificate for the Orchestrator configuration interface, or the SSL certificate for the Orchestrator client.
**Change the Certificate of the Orchestrator Appliance Management Site**

The Orchestrator Appliance uses light-httpd to run its own management site. You can change the SSL certificate of the Orchestrator Appliance management site, for example if your company security policy requires you to use its SSL certificates.

**Prerequisites**

By default the Orchestrator Appliance SSL certificate and private key are stored in a PEM file, which is located at: `/opt/vmware/etc/lighttpd/server.pem`. To install a new certificate, ensure that you export your new SSL certificate and private key from the Java keystore to a PEM file.

**Procedure**

1. Log in to the Orchestrator Appliance Linux console as root.
2. Locate the `/opt/vmware/etc/lighttpd/lighttpd.conf` file and open it in an editor.
3. Find the following line:
   ```
   #### SSL engine
   ssl.engine = "enable"
   ssl.pemfile = "/opt/vmware/etc/lighttpd/server.pem"
   ```
4. Change the `ssl.pemfile` attribute to point to the PEM file containing your new SSL certificate and private key.
5. Save the `lighttpd.conf` file.
6. Run the following command to restart the light-httpd server.
   ```
   service vami-lighttp restart
   ```

You successfully changed the certificate of the Orchestrator Appliance management site.

**Change the Web Views 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.

**Prerequisites**

Make sure that you have generated or installed an SSL certificate signed by a CA.

**Procedure**

1. Open the `server.xml` configuration file in a text editor.
   The default location is:
   ```
   /opt/vmo/app-server/server/vmo/deploy/jboss-deploy-tomcat/jbossweb-tomcat55.sar/server.xml
   ```
2. Find the following entry in the `server.xml` file.
   ```
   <!-- Define a SSL HTTP/1.1 Connector on port ${ch.dunes.https-server.port} -->
   <Connector address="${jboss.bind.address}" protocol="HTTP/1.1" SSLEnabled="true"
   clientAuth="false" emptySessionPath="true"
   keystoreFile="${java.home}/lib/security/jssecacerts"
   keystorePass="dunesdunes"
   ```
3  Change the keystoreFile and keystorePass attributes to refer to the `<your_keystore_filename>` file and the password you created when you ran the keytool utility.

```java
keystoreFile="/PathToKeystore/<your_keystore_filename>
keystorePass="NewKeystorePassword"
```

The keystoreFile attribute should contain slashes as directory separators.

4  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.

---

### Change the SSL Certificate of the Orchestrator Configuration Interface

You can configure the Orchestrator configuration server to use a different SSL certificate, for example if your company security policy requires you to use their SSL certificates.

**Prerequisites**

Make sure that you have generated or installed an SSL certificate signed by a CA.

**Procedure**

1  Log in to the appliance Linux console as root and navigate to the jetty.xml file.

   The default location is:

   `/opt/vmo/configuration/jetty/etc/jetty.xml`.

2  In the jetty.xml file, find the following entry:

   ```xml
   <Call name="addConnector">
   <Arg>
   <New class="org.mortbay.jetty.security.SslSocketConnector">
   <Set name="Port">8283</Set>
   <Set name="maxIdleTime">30000</Set>
   <Set name="handshakeTimeout">2000</Set>
   <Set name="keystore">/<SystemProperty name="jetty.home" default="."="/etc/jssecacerts</Set>
   <Set name="password">dunesdunes</Set>
   <Set name="keyPassword">dunesdunes</Set>
   <Set name="truststore">/<SystemProperty name="jetty.home" default="."="/etc/jssecacerts</Set>
   <Set name="trustPassword">dunesdunes</Set>
   ```

3  Change the keystore, truststore, password, keyPassword and trustPassword values to refer to your `<your_keystore_filename>` file and password.

4  Save the jetty.xml file.

5  Restore the default vco user credentials by running the following command:

   ```bash
   chown vco.vco /opt/vmo/configuration/jetty/etc/jetty.xml
   chmod 600 /opt/vmo/configuration/jetty/etc/jetty.xml
   ```

   **IMPORTANT**  The vco user must be the owner of the jetty.xml file. Otherwise you cannot start the Orchestrator configuration service.

6  Restart the Orchestrator configuration server.

You successfully changed the SSL certificate for the Orchestrator configuration interface.
Change the SSL Certificate for the Orchestrator Client

By default, the Orchestrator server uses the predefined SSL certificate to communicate remotely with the Orchestrator client. You can change the SSL certificate for the Orchestrator client, for example if your company security policy requires you to use its SSL certificates.

Prerequisites

Make sure that you have generated or installed an SSL certificate signed by a CA.

Procedure

1. Open the following Orchestrator application server service file in a text editor.
   The default location is:
   `/opt/vmo/app-server/server/vmo/conf/jboss-service.xml`

2. Find the following entry in the `jboss-service.xml` file.
   ```xml
   <!-- The SSL domain setup -->
   <mbean code="org.jboss.security.plugins.JaasSecurityDomain"
      name="Security:name=JaasSecurityDomain,domain=dunes">
     <constructor>
      <arg type="java.lang.String" value="dunes"/>
     </constructor>
     <attribute name="KeyStoreURL">${java.home}/lib/security/jssecacerts</attribute>
     <attribute name="KeyStorePass">dunesdunes</attribute>
   </mbean>
   ```

3. Change the `keystoreURL` and `keystorePass` attributes to refer to the path to the `your_keystore_filename` file and the password you created when you ran the `keytool` utility.
   ```xml
   keystoreURL="/PathToKeystore/<your_keystore_filename>"
   keystorePass="NewKeystorePassword"
   ```
   The `keystoreURL` attribute is a URL and must contain slashes as directory separators.

4. Save the `jboss-service.xml` file and restart the Orchestrator server.

   The Orchestrator client authenticates the Orchestrator server by using the SSL certificate you changed.
The Orchestrator client is an easy-to-use desktop application that you can use to perform daily administration tasks such as importing packages, running and scheduling workflows, and managing user permissions. The Orchestrator client also serves as an IDE for creating or customizing workflows.

For more information about using the Orchestrator client interface and how to create workflows, actions, packages, and other custom Orchestrator elements, see *Using the VMware vCenter Orchestrator Client* and *Developing with VMware vCenter Orchestrator*.

The Web operator provides an example of the orchestration functions that Web views can provide to end users in browsers, without requiring that those users use the Orchestrator client.

With the Orchestrator Web operator, you can run and monitor workflows in a Web browser without logging in to the Orchestrator client interface.

This chapter includes the following topics:

- “Log In to the Orchestrator Client,” on page 43
- “Log In to the Orchestrator Web Operator,” on page 44
- “Download and Install the Orchestrator Client,” on page 45

### Log In to the Orchestrator Client

To perform general administration tasks or to edit and create workflows, you must log in to the Orchestrator client interface.

The Orchestrator client interface is designed for developers with administrative rights who want to develop workflows, actions, and other custom elements.

**IMPORTANT** Ensure that the clocks of the Orchestrator Appliance and the Orchestrator client machine are synchronized.

**Prerequisites**

- Download and deploy the Orchestrator Appliance.
- Ensure that the appliance is up and running.

**Procedure**

1. In a Web browser, navigate to the IP address that your Orchestrator Appliance virtual machine provides.
   
   http://orchestrator_appliance_ip

2. Click **Start Orchestrator Client**.
3 Type the IP or the domain name of the Orchestrator Appliance in the **Host name** text box. The IP address of the Orchestrator Appliance is displayed by default.

4 Log in by using the Orchestrator client user name and password. The default OpenLDAP credentials are:

- User name: `vcoadmin`
- Password: `vcoadmin`

If you are using vCenter Single Sign On or another directory service as an authentication method, type the respective credentials to log in to the Orchestrator client.

5 In the Security Warning window select an option to handle the certificate warning.
The Orchestrator client communicates with the Orchestrator server by using an SSL certificate. A trusted CA does not sign the certificate during installation. You receive a certificate warning each time you connect to the Orchestrator server.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ignore</td>
<td>Continue using the current SSL certificate. The warning message appears again when you reconnect to the same Orchestrator server, or when you try to synchronize a workflow with a remote Orchestrator server.</td>
</tr>
<tr>
<td>Cancel</td>
<td>Close the window and stop the login process.</td>
</tr>
<tr>
<td>Install this certificate and do not display any security warnings for it anymore.</td>
<td>Select this check box and click <strong>Ignore</strong> to install the certificate and stop receiving security warnings.</td>
</tr>
</tbody>
</table>

You can change the default SSL certificate with a certificate signed by a CA. For more information about changing SSL certificates, see *Installing and Configuring VMware vCenter Orchestrator*.

**What to do next**

You can import a package, start a workflow, or set root access rights on the system. See *Using the VMware vCenter Orchestrator Client*.

**Log In to the Orchestrator Web Operator**

To run and schedule workflows from the Orchestrator Web operator, you must first log in.

**Prerequisites**

- Download and deploy the Orchestrator Appliance.
- Ensure that the appliance is up and running.

**Procedure**

1 In a Web browser, navigate to the IP address that your Orchestrator Appliance virtual machine provides.

   http://orchestrator_appliance_ip

2 Click **Web Operator**.

3 Log in by using the Orchestrator user name and password. The default credentials are:

   - User name: `vcoadmin`
Password: vcoadmin

If you are using vCenter Single Sign On or another directory service as an authentication method, type the respective credentials to log in to the Orchestrator client.

You see the workflow library tree and you can run and monitor workflow runs.

Download and Install the Orchestrator Client

If you want to use the Orchestrator client to connect to the Orchestrator server not through the Java Web Start, but to have the client installed on your local machine, you must download and install the Orchestrator client.

After you complete the installation, you can start the Orchestrator client and connect to the Orchestrator server installed with the Orchestrator Appliance.

**IMPORTANT** Ensure that the clocks of the Orchestrator Appliance and the Orchestrator client machine are synchronized.

**Prerequisites**

- Download and deploy the Orchestrator Appliance.
- Ensure that the appliance is up and running.

**Procedure**

1. In a Web browser, navigate to the IP address that your Orchestrator Appliance virtual machine provides. http://orchestrator_appliance_ip
2. Click **Download vCenter Orchestrator Client installable**.
   You see links to executables for Windows 64-bit and 32-bit, Linux 64-bit, and Mac.
3. Download the file suitable for your operating system and install the Orchestrator client.

**What to do next**

Start the Orchestrator client on your machine and log in by using the Orchestrator client user name and password. The default credentials are:

- **User name:** vcoadmin
- **Password:** vcoadmin

If you are using vCenter Single Sign On or another directory service as an authentication method, type the respective credentials to log in to the Orchestrator client.
# Index

## A
- assign static IP 16
- audience 5
- authentication type 26

## C
- change the management site SSL certificate 39
- change vCO appliance password 16
- check-pointing 7
- configuration
  - database connection 36
  - LDAP settings 32
- configuring
  - network settings 16
  - Orchestrator server 21
  - proxy settings 16
  - update checks 18
- configuring the vCO appliance 15

## D
- database
  - connection parameters 36
  - import SSL certificate 35
  - installation 34
- Oracle 34
- server size 34
- setup 34
- SQL Server 34
  - SQL Server Express 34
- deploy the Orchestrator appliance 12
- dereference links 34
- disable SSH login 16
- download the Orchestrator appliance 12

## E
- enable SSH login 16

## F
- filter attributes 34

## G
- generate a certificate 37
- get a certificate signed by a CA 38

## I
- ignore referrals 34
- import SSL certificate, vCenter Single Sign  
  - On 27
- install, SSL certificate from a CA 38
- install updates 18

## L
- LDAP
  - browsing credentials 32
  - connection URL 30
  - LDAP Server Signing Requirements 30
  - lookup paths 32
  - SSL certificate 30
- LDAP server 29
- license, importing vCenter Server license 22
- log in to
  - Linux console 13
  - Orchestrator client 43
  - Orchestrator configuration 22
  - Web console 15
  - Web operator 44

## N
- non-ASCII characters 36

## O
- Orchestrator appliance
  - configure for updates 18
  - deploy 12
  - download 12
  - overview 11
  - update 17
  - version status 17
- Orchestrator architecture 9
- Orchestrator client
  - change the SSL certificate 41
  - start 45
- Orchestrator client overview 43
- Orchestrator client, download 45
- Orchestrator client, install 45
- Orchestrator configuration, log in 22
- Orchestrator configuration interface, change SSL certificate 40
- Orchestrator overview 7
- Orchestrator plug-ins 10
Orchestrator version 11
OS 11
overview of, vCenter Single Sign On 26

P
persistence 7
plug-ins configuration, vCenter Server plug-in 24,
25
policy engine 7
power on 13

S
scripting engine 7
security 7
SSH login 16
SSL certificate 24
SSL certificate, import 27
SSL certificates 37

T
timeouts 34

U
user permissions 26
user roles 8

V
vCenter Server plug-in, install 24
vCenter Single Sign On
advanced registration 28
import SSL certificate 27
simple registration 28
vCO appliance
change password 16
configuring 15
versioning 7

W
Web console, log in 15
Web operator 43
Web views, change SSL certificate 39
workflow engine 7