Installing and Configuring VMware vRealize Orchestrator

vRealize Orchestrator 6.0.1

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.

EN-001378-01

vmware®

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

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

The VMware Web site also provides the latest product updates.

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

docfeedback@vmware.com

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

Contents

Installing and Configuring VMware vRealize Orchestrator

Installing and Configuring VMware vRealize Orchestrator provides information and instructions about installing, upgrading and configuring VMware® vRealize Orchestrator.

Intended Audience

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

Updated Information

Installing and Configuring VMware vRealize Orchestrator is updated with each release of the product or when necessary.

This table provides the update history of the *Installing and Configuring VMware vRealize Orchestrator*.

Revision	Description
EN-001378-01	■ In "Log in to the Orchestrator Client on a Windows Machine," on page 121, added information about the default Orchestrator user name and password. ■ Updated the "Configuring a Cluster of Orchestrator Server Instances," on page 67 topic. ■ Created the "Configuring a Load Balancer," on page 68, "Configure the NSX Load Balancer to Work With an Orchestrator Cluster," on page 69, and "Configure the F5 Load Balancer to Work With an Orchestrator Cluster," on page 70 topics. ■ Updated information about the default vCenter Orchestrator instance in "Setting Up Orchestrator to Work with the vSphere Web Client," on page 100
EN-001378-00	Initial release.

Introduction to VMware vRealize Orchestrator 1

VMware vRealize 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

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 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.

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 global user roles. In Orchestrator, you can have users with full rights, that are a part of the administrator group (Administrators) and users with limited rights, that are not part of the administrator group (End Users).

Users with Full Rights

Orchestrator administrators and developers have equal administrative rights, but are divided in terms of responsibilities.

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
- 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

Users with Limited Rights

End Users

End users can run and schedule workflows and policies that the administrators or developers make available in the Orchestrator client.

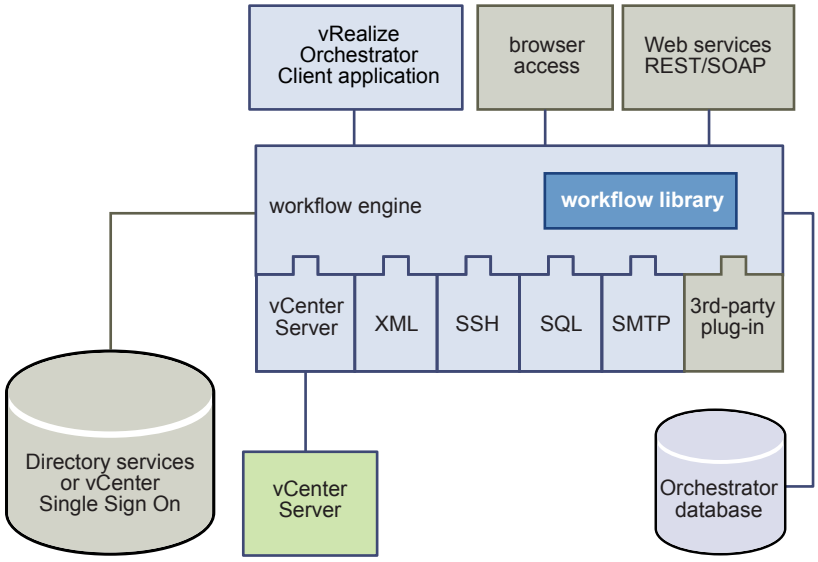
Orchestrator Architecture

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 an authentication provider 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, or through Web services.

Figure 1-1. VMware vRealize Orchestrator Architecture



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. For more information about the Orchestrator plug-ins that VMware develops and distributes, see http://www.vmware.com/support/pubs/vco_plugins_pubs.html. For more information about third-party Orchestrator plug-ins, see https://solutionexchange.vmware.com/store/vco.

Orchestrator System Requirements 2

Your system must meet the technical requirements that are necessary for Orchestrator to work properly.

For a list of the supported versions of vCenter Server, the vSphere Web Client, vCloud Automation Center, and other VMware solutions, as well as compatible database versions, see VMware Product Interoperability Matrix.

This chapter includes the following topics:

Hardware Requirements for Orchestrator

Verify that your system meets the minimum hardware requirements before you install Orchestrator.

- 2.0 GHz or faster Intel or AMD x64 processor. At least two CPUs are recommended. Processor requirements might differ if your database runs on the same hardware.
- 4 GB RAM. You might need more RAM if your database runs on the same hardware.
- 4 GB disk space. You might need more storage if your database runs on the same hardware.
- A free static IP address.

Hardware Requirements for the Orchestrator Appliance

The Orchestrator Appliance is a preconfigured Linux-based virtual machine. Before you deploy the appliance, verify that your system meets the minimum hardware requirements.

The Orchestrator Appliance has the following hardware configuration:

- 2 CPUs
- 3 GB of memory

- 12 GB hard disk

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

Operating Systems Supported by Orchestrator

You can install the Orchestrator server only on 64-bit operating systems.

Orchestrator is also available as a virtual appliance running on a SUSE Linux Enterprise Server.

For a list of the operating systems supported by Orchestrator, see Supported host operating systems for VMware vCenter Server installation.

Supported Directory Services

If you plan to use an LDAP server for authentication, ensure that you set up and configure a working LDAP server.

NOTE LDAP authentication is deprecated.

Orchestrator supports these directory service types.

- Windows Server 2008 Active Directory
- Windows Server 2012 Active Directory
- OpenLDAP
- Novell eDirectory Server 8.8.3
- Sun Java System Directory Server 6.3

IMPORTANT Multiple domains that have a two-way trust, but are not in the same tree, 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.

Browsers Supported by Orchestrator

The Orchestrator configuration interface requires a Web browser.

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

- Microsoft Internet Explorer 10 or later
- Mozilla Firefox
- Google Chrome

Orchestrator Database Requirements

The Orchestrator server requires a database. For small-scale deployments, you can use the preconfigured Orchestrator database. For better performance in a production environment, use a separate database for Orchestrator.

NOTE To ensure efficient CPU and memory usage, consider hosting the Orchestrator database and the Orchestrator server on different machines. Verify that at least 1 GB of free disk space is available on each machine.

For a list of the supported database versions, see VMware Product Interoperability Matrix.

Software Included in the Orchestrator Appliance

The Orchestrator Appliance is a preconfigured virtual machine optimized for running Orchestrator. The appliance is distributed with preinstalled software.

The Orchestrator Appliance package contains the following software:

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

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, you must 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, see "Selecting the Authentication Type," on page 42. For information about configuring a database for production environments, see "Setting Up the Orchestrator Database," on page 20.

NOTE LDAP authentication is deprecated.

Level of Internationalization Support

Orchestrator supports internationalization level 1.

Non-ASCII Character Support in Orchestrator

Although Orchestrator is not localized, it can run on a non-English operating system and support non-ASCII text.

Table 2-1. Non-ASCII Character Support in Orchestrator GUI

	Support for Non-ASCII Characters			
Orchestrator Item	**Description Field**	**Name Field**	**Input and Output Parameters**	**Attributes**
Action	Yes	No	No	No
Folder	Yes	Yes	-	-
Configuration element	Yes	Yes	-	No
Package	Yes	Yes	-	-
Policy	Yes	Yes	-	-
Policy template	Yes	Yes	-	-
Resource element	Yes	Yes	-	-
Workflow	Yes	Yes	No	No
Workflow presentation display group and input step	Yes	Yes	-	-

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.

Setting Up Orchestrator Components 3

You can install Orchestrator on a computer running Microsoft Windows or you can download and deploy the Orchestrator Appliance. In both cases, the Orchestrator server is preconfigured, and after successful installation or deployment, the service starts automatically.

To enhance the availability and scalability of your Orchestrator setup, you can follow several guidelines :

- Install Orchestrator on a computer different from the computer on which vCenter Server runs.
- Install and configure a database and configure Orchestrator to connect to it.
- Install and configure a VMware vCenter Single Sign-On server and configure Orchestrator to work with it.

This chapter includes the following topics:

Orchestrator Configuration Maximums

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

Table 3-1. Orchestrator Configuration Maximums

Item	Maximum
Connected vCenter Server systems	20
Connected ESX/ESXi servers	1280
Connected virtual machines spread over vCenter Server systems	35000
Concurrent running workflows	300

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 100 Mb line is mandatory.

Authentication Methods

To authenticate and manage user permissions, Orchestrator requires a connection to an LDAP server or a connection to a Single Sign-On server.

Orchestrator supports the Active Directory, OpenLDAP, eDirectory, and Sun Java System Directory Server directory service types.

NOTE LDAP authentication is deprecated.

If you download and deploy the Orchestrator Appliance, the Orchestrator server is preconfigured to work with the OpenLDAP server distributed together with the appliance. The default OpenLDAP configuration is suitable for small- or medium-scale environment. To use Orchestrator in a production environment, you must set up either an LDAP server or a vCenter Single Sign-On server and configure Orchestrator to work with it.

To use LDAP server, you must 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. The resources that you need depend on the combination of database and directory service you choose. For recommendations, see the documentation for your LDAP server.

To use the vCenter Single Sign-On authentication method, you must first install vCenter Single Sign-On. You must configure the Orchestrator server to use the vCenter Single Sign-On server that you installed and configured.

To use Single Sign-On authentication through vCloud Automation Center, you must run the Register Orchestrator in vCloud Automation Center component registry workflow in the Orchestrator client.

Setting Up the Orchestrator Database

Orchestrator requires a database to store workflows and actions.

The Orchestrator server is preconfigured to use an embedded database, which is suitable for testing purposes only. You must configure Orchestrator to use a separate database by using the Orchestrator configuration interface. When the database is embedded, you cannot set up Orchestrator to work in cluster mode, or change the license and the server certificate from the Orchestrator configuration interface. To change the server certificates without changing the database settings, you must run the configuration workflows by using either the Orchestrator client or the REST API. For more information about running the configuration workflows by using the Orchestrator client, see *Using the VMware vRealize OrchestratorPlug-Ins*. For detailed instructions about running the configuration workflows by using the REST API, see Chapter 7, "Configuring Orchestrator by Using the Configuration Plug-In and the REST API," on page 79.

To use Orchestrator in a production environment, you must configure the Orchestrator server to use a dedicated Orchestrator database.

If you download and deploy the Orchestrator Appliance, the Orchestrator server is preconfigured to work with the PostgreSQL database distributed with the appliance. The default Orchestrator Appliance database configuration is suitable for small- or medium-scale environment. To use Orchestrator in a production environment, you must set up a database and configure Orchestrator to work with it.

Orchestrator server supports Oracle, Microsoft SQL Server, and PostgreSQL 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 52.

The common workflow for setting up the Orchestrator database consists of the following steps:

1 Create a new database. For more information about creating a new database, see the documentation of your database provider.

2 Enable the database for remote connection. For an example, see "Configure SQL Server Express to Use with Orchestrator," on page 52.

3 Configure the database connection parameters. For more information, see "Configuring the Orchestrator Database Connection," on page 52.

If you plan to set up an Orchestrator cluster, you must configure the database to accept multiple connections so that it can accept connections from the different Orchestrator server instances in the cluster.

The database setup can affect Orchestrator performance. Install the database on a machine other than the one on which the Orchestrator server is installed. This approach ensures that the JVM and database server do not share CPU, RAM, and I/O.

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 geographically closest to your Orchestrator server and that is on the network with the highest available bandwidth.

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

CAUTION Verify that at least 1 GB of 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 cause the Orchestrator server and client to not function correctly.

Installing and Upgrading Orchestrator

4

Orchestrator consists of a server component and a client component. You can download and deploy the Orchestrator Appliance or install Orchestrator standalone on a Windows machine.

You can install the Orchestrator configuration server on 64-bit Windows machines only. The Orchestrator client can run on 64-bit Windows, Linux, and Mac machines.

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

To use Orchestrator, you must start the Orchestrator Server service and then start the Orchestrator client.

If you need to change the default Orchestrator configuration settings, you can start the Orchestrator Configuration service and change the settings by using the Orchestrator configuration interface. You can also run the Orchestrator configuration workflows by using either the Orchestrator client or the REST API.

This chapter includes the following topics:

Install Orchestrator Standalone

For production environments and to enhance the scalability of your Orchestrator setup, install Orchestrator on a dedicated Windows machine.

The Orchestrator client and server can run on 64-bit Windows machines.

NOTE If you try to install Orchestrator on a 64-bit machine on which an instance of Orchestrator 4.0.x is running, the 64-bit installer does not detect the earlier version of Orchestrator. As a result, two versions of Orchestrator are installed and coexist.

Prerequisites

- Verify that your hardware meets the Orchestrator system requirements. See "Hardware Requirements for Orchestrator," on page 15.
- Download the vRealize Orchestrator installer from the VMware Web site.

Procedure

1 Start the Orchestrator installer.

Browse to the download location of the installer and start vRealizeOrchestrator-6.0.0.exe

2 Click **Next**.

3 Accept the terms in the license agreement and click **Next**.

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

CAUTION You cannot install Orchestrator in a directory whose name contains non-ASCII characters. If you are operating in a locale that features non-ASCII characters, you must install Orchestrator in the default location.

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

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

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

CAUTION The name of the shortcuts directory must contain only ASCII characters.

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

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

What to do next

To start configuring Orchestrator, start the VMware vRealize Orchestrator Configuration service and log in to the Orchestrator configuration interface at: https://*orchestrator_server_DNS_name_or_IP_address*:8283/vco-config or https://localhost:8283/vco-config.

Install the Client Integration Plug-In

The Client Integration Plug-in provides access to a virtual machine's console in the vSphere Web Client, and provides access to other vSphere infrastructure features.

You use the Client Integration Plug-in to deploy OVF or OVA templates and transfer files with the datastore browser. You can also use the Client Integration Plug-in to connect virtual devices that reside on a client computer to a virtual machine.

Install the Client Integration Plug-in only once to enable all the functionality the plug-in delivers. You must close the Web browser before installing the plug-in.

If you install the Client Integration Plug-in from an Internet Explorer browser, you must first disable Protected Mode and enable pop-up windows on your Web browser. Internet Explorer identifies the Client Integration Plug-in as being on the Internet instead of on the local intranet. In such cases, the plug-in is not installed correctly because Protected Mode is enabled for the Internet.

You cannot launch the virtual machine console in Internet Explorer without the Client Integration Plug-in. In other supported browsers, the virtual machine console can run without the plug-in.

The Client Integration Plug-in also lets you log in to the vSphere Web Client by using Windows session credentials.

For information about supported browsers and operating systems, see the *vSphere Installation and Setup* documentation.

Watch the video "Installing the Client Integration Plug-In" for information about the Client Integration Plug-In:

Installing the Client Integration Plug-In
(http://link.brightcove.com/services/player/bcpid2296383276001?bctid=ref:video_client_plug_in)

Prerequisites

If you use Microsoft Internet Explorer, disable Protected Mode.

Procedure

1 In the vSphere Web Client, navigate to a link to download the Client Integration Plug-in.

Option	Description
vSphere Web Client login page	a Open a Web browser and type the URL for the vSphere Web Client. b At the bottom of the vSphere Web Client login page, click **Download Client Integration Plug-in**.
Guest OS Details panel	This option is not available for browsers that run on a Mac OS. a Select a virtual machine in the inventory and click the **Summary** tab. b Click **Download Plug-in**.
OVF deployment wizard	a Select a host in the inventory and select **Actions > All vCenter Actions > Deploy OVF Template**. b Click **Download Client Integration Plug-in**.
Virtual machine console	This option is not available for Microsoft Internet Explorer, and for browsers that run on a Mac OS. a Select a virtual machine in the inventory, click the **Summary** tab, and click **Launch Console**. b At the top right corner of the virtual machine console window, click **Download Client Integration Plugin**.

2 If the browser blocks the installation either by issuing certificate errors or by running a pop-up blocker, follow the Help instructions for your browser to resolve the problem.

Download and Deploy the Orchestrator Appliance

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

Prerequisites

Verify that your computing environment meets the following conditions:

- vCenter Server is installed and running.
- The host on which you are deploying the appliance has enough free disk space.
- The Client Integration plug-in is installed before you deploy an OVF template. This plug-in enables OVF deployment on your local file system.

If your system is isolated and without Internet access, you must download either the `.vmdk` and `.ovf` files, or the `.ova` file for the appliance from the VMware Web site, and save the files in the same folder.

Procedure

1 Log in to the vSphere Web Client as an administrator.

2 In the vSphere Web Client, select an inventory object that is a valid parent object of a virtual machine, such as a datacenter, folder, cluster, resource pool, or host.

3 Select **Actions > Deploy OVF Template**.

4 Type the path or the URL to the `.ovf` or `.ova` file and click **Next**.

5 Review the OVF details and click **Next**.

6 Accept the terms in the license agreement and click **Next**.

7 Type a name and location for the deployed appliance, and click **Next**.

8 Select a host, cluster, resource pool, or vApp as a destination on which you want the appliance to run, and click **Next**.

9 Select a format in which you want to save the appliance's virtual disk and the storage.

Format	Description
Thick provisioned Lazy Zeroed	Creates a virtual disk in a default thick format. The space required for the virtual disk is allocated when the virtual disk is created. If any data remains on the physical device, it is not erased during creation, but is zeroed out on demand later on first write from the virtual machine.
Thick Provisioned Eager Zeroed	Supports clustering features such as Fault Tolerance. The space required for the virtual disk is allocated when the virtual disk is created. If any data remains on the physical device, it is zeroed out when the virtual disk is created. It might take much longer to create disks in this format than to create disks in other formats.
Thin provisioned format	Saves storage space. For the thin disk, you provision as much datastore space as the disk requires based on the value that you select for the disk size. The thin disk starts small and at first, uses only as much datastore space as the disk needs for its initial operations.

10 (Optional) Configure the network settings, 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.

11 Review the properties of the appliance and set initial passwords for the root user account and for the vmware user in the Orchestrator Configuration interface.

Your initial passwords must be at least eight characters long, and must contain at least one digit, special character, and uppercase letter.

IMPORTANT The password for the root account of the Orchestrator Appliance expires after 365 days. You can increase the expiry time for an account by logging in to the Orchestrator Appliance as root, and running `passwd –x number_of_days name_of_account`. If you want to increase the Orchestrator Appliance root password to infinity, run `passwd –x 99999 root`.

12 Review the Ready to Complete page and click **Finish**.

The Orchestrator Appliance is successfully deployed.

Power On the Orchestrator Appliance and Open the Home Page

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

Procedure

1 Log in to the vSphere Web Client as an administrator.

2 Right-click the Orchestrator Appliance and select **Power > Power On**.

3 On the **Summary** tab, view the Orchestrator Appliance IP address.

4 In a Web browser, go to the IP address of your Orchestrator Appliance virtual machine.

http://*orchestrator_appliance_ip*

Change the Root Password

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

IMPORTANT The password for the root account of the Orchestrator Appliance expires after 365 days. You can increase the expiry time for an account by logging in to the Orchestrator Appliance as root, and running `passwd –x number_of_days name_of_account`. If you want to increase the Orchestrator Appliance root password to infinity, run the `passwd –x 99999 root` command.

Prerequisites

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

Procedure

1 In a Web browser, go to https://*orchestrator_appliance_ip*:5480.

2 Type the appliance user name and password.

3 Click the **Admin** tab.

4 In the **Current administrator password** text box, type the current root password.

5 Type the new password in the **New administrator password** and **Retype new administrator password** text boxes.

6 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 vRealize 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.
- Verify that the appliance is up and running.

Procedure

1 In a Web browser, go to https://*orchestrator_appliance_ip*:5480.

2 Log in as root.

3 On the **Admin** tab, click **Toggle SSH setting** to allow log in as root to the Orchestrator Appliance using SSH.

4 (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 address and define the proxy settings.

Prerequisites

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

Procedure

1 In a Web browser, go to https://*orchestrator_appliance_ip*:5480.

2 Log in as root.

3 On the **Network** tab, click **Address**.

4 Select the method by which the appliance obtains IP address settings.

Option	Description
DHCP	Obtains IP settings from a DHCP server. This is the default setting.
Static	Uses static IP settings. Type the IP address, netmask, and gateway.

Depending on your network settings, you might have to select IPv4 and IPv6 address types.

5 (Optional) Type the necessary network configuration information.

6 Click **Save Settings**.

7 (Optional) Set the proxy settings and click **Save Settings**.

Upgrade Orchestrator Standalone

To upgrade Orchestrator on a 64-bit Microsoft Windows machine that is different from the machine on which vCenter Server runs, run the latest version of the Orchestrator standalone installer.

Prerequisites

- Create a backup of the Orchestrator database.
- Back up your Orchestrator configuration, custom workflows, and packages. See "Back Up the Orchestrator Configuration and Elements," on page 108.
- Log in as Administrator to the Windows machine on which you are performing the upgrade.
- Download the vRealize Orchestrator installer from the VMware Web site.

Procedure

1 Stop the Orchestrator server services.

   a Select **Start > Programs > Administrative Tools > Services**.

   b In the right pane, right-click **VMware vRealize Orchestrator Server** and select **Stop**.

   c In the right pane, right-click **VMware vRealize Orchestrator Configuration** and select **Stop**.

2 (Optional) Back up your Orchestrator plug-in files and their configurations so that you can import them after the upgrade.

Option	Action
To back up the plug-ins	Copy the files from *`install_directory`*`\VMware\Orchestrator\app-server\plugins` to your backup location.
To back up the plug-in configurations	Copy the files from *`install_directory`*`\VMware\Orchestrator\app-server\conf\plugins` to your backup location.

3 Start the Orchestrator installer.

   Browse to the download location of the installer and start vRealizeOrchestrator-6.0.0.exe

4 Click **Next**.

5 Accept the terms in the license agreement and click **Next**.

6 Select **Continue with update** to upgrade Orchestrator.

7 After the installer detects the installation directory, click **Next** .

   You cannot change the installation directory when you are upgrading Orchestrator. To change this parameter, you must perform a new installation.

8 Select the upgrade that matches your existing Orchestrator installation and click **Next**.

Option	Description
Client	Upgrades the Orchestrator client application.
Server	Upgrades the Orchestrator server platform.
Client-Server	Upgrades the Orchestrator client and server.

   For example, if you have installed only the Orchestrator client, select **Client** and then upgrade your Orchestrator server separately.

   IMPORTANT The versions of the Orchestrator client and server must be the same.

9 Select the location for the Orchestrator shortcuts and click **Next**.

CAUTION The name of the shortcuts directory must contain only ASCII characters.

10 Click **Install** to start the installation process.

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

12 (Optional) Import the backed up plug-in files to your new Orchestrator version.

Option	Action
To import the plug-ins	Copy the backed up files to *install_directory*\VMware\Orchestrator\app-server\plugins.
To import the plug-in configurations	Copy the backed up files to *install_directory*\VMware\Orchestrator\app-server\conf\plugins.

Orchestrator automatically upgrades the plug-ins that are installed with it by default. Import only changed plug-in files.

13 Start the Orchestrator configuration service and log in to the Orchestrator configuration interface.

14 Reimport the SSL certificate for the licensed vCenter Server and start the Orchestrator server.

15 On the **Plug-ins** tab, click **Reload all plug-ins**.

16 On the **Startup Options** tab, click **Restart the vRO configuration server**.

17 Click **Start service** to start the Orchestrator server.

You upgraded to the latest version of Orchestrator. The existing Orchestrator configuration is preserved.

Create an Archive for Upgrading Orchestrator

If you upgrade Orchestrator by upgrading vCenter Server 5.0 or later to vCenter Server 6.0, the `vco_export.zip` archive, located at `%VMWARE_CIS_HOME%/vco` might not get created automatically and your configuration might not be migrated.

Problem

During the export phase of the upgrade, Orchestrator upgrade script collects configuration files and data, and stores them in the `vco_export.zip` archive. In some cases the archive might not be created automatically and must be created manually if you want to preserve the data after the update.

Cause

During an export, Orchestrator accesses the Windows registry to find the necessary data. If Orchestrator cannot access that data, the automatic export does not occur.

Solution

1 Create the `vco_export.zip` archive manually with the necessary data, and save it to `%VMWARE_CIS_HOME%/vco`.

The export archive must contain the following files:

File	Location	Description
Plug-in DAR files	■ On Orchestrator 5.5.x: *install_directory*\VMware\Orchestrator\app-server\plugins ■ On Orchestrator 5.1 or earlier: *install_directory*\VMware\Orchestrator\app-server\server\vmo\plugins	A copy of the plug-in `.dar` files. During the import phase, plug-ins are not downgraded. Orchestrator imports only the plug-in configuration but a `.dar` file is not substituded by an earlier version. If a source plug-in is not installed on the destination system, it is imported and disabled. Source plug-ins might not be verified for Orchestrator 6.0.1 and might cause errors.
`vmo_config.zip`	The location varies. After you export the file, you receive a message with the location of the file.	This file has the same content as the `.vmoconfig` file generated by the Orchestrator Configuration's **Export Configuration** option found on the **General** tab.

File	Location	Description
Properties files	■ On Orchestrator 5.5.x: *install_directory*\VMware\Orchestrator\app-server\conf ■ On Orchestrator 5.1 or earlier: *install_directory*\VMware\Orchestrator\app-server\server\vmo\conf	All of the `.properties` files located in the folder. The folder may also include custom defined properties. The file `sso.properties` is present only if the source system is configured to use Single Sign-On.
`jssecacerts`	On Orchestrator 4.2.x: *install_directory*\VMware\Orchestrator\jre\lib\security\jssecacerts	This file is included only in Orchestrator 4.2.x. In later versions, the file is a part of `vmo_config.zip`. It contains the Certificate Authorities certificates, which are imported through the Orchestrator configuration interface.

2 Use the archive to migrate your configuration.

a Log in to the Orchestrator configuration interface as **`vmware`**.

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

c Type the password you used when exporting the configuration.

This step is not necessary if you have not specified a password.

d Browse to select the `vco_export.zip` file.

e Select whether to override the Orchestrator internal certificate and network settings.

Select the check box only if you want to restore your Orchestrator configuration and the `vco_export.zip` file is the backup file of the same Orchestrator configuration.

If you import the configuration to duplicate the Orchestrator environment, for example for scaling purposes, leave the check box unselected. Otherwise you might have problems with the certificates when Orchestrator tries to identify against vCenter Server, vCenter Single Sign-On or the vSphere Web Client.

f Click **Import**.

Upgrade Orchestrator Appliance 5.5.x to 6.0.1

You can upgrade Orchestrator Appliance 5.5.x to 6.0.1 with packages that VMware publishes. You must perform the upgrade through the Orchestrator Appliance configuration portal.

You can upgrade your existing Orchestrator Appliance 5.5.x to 6.0.1 by using the Orchestrator Appliance configuration portal on port 5480. After you upgrade the Orchestrator Appliance, your plug-in settings are preserved.

Prerequisites

Unmount all network file systems.

Procedure

1 Access the VMware vRealize Orchestrator Appliance configuration portal at https://*orchestrator_server*:5480/.

2 Log in to the Orchestrator Appliance configuration portal as an administrator.

3 On the **Update** tab, click **Check Updates**.

The system checks for available updates.

4 If any updates are available, click **Install Updates**.

To proceed with the upgrade, you must accept the VMware End User License Agreement.

5 To complete the update, restart the Orchestrator Appliance.

6 (Optional) On the **Update** tab, verify that Orchestrator Appliance 6.0.1 has been successfully installed.

7 If there are any changes to the vCenter Server certificates during the upgrade of vCenter Server, you must import the correct vCenter Server certificates and restart the Orchestrator Appliance.

You have successfully upgraded the Orchestrator Appliance to version 6.0.1.

What to do next

Verify that the Orchestrator Appliance vco user account has sufficient permissions for all custom files and folders.

Import the SSL certificates for each vCenter Server instance that you defined. See "Import the vCenter Server SSL Certificate," on page 41.

Upgrading Orchestrator Appliance 5.5 and Earlier

To upgrade Orchestrator Appliance with version 5.5 or earlier to 6.0, you must deploy the latest Orchestrator Appliance and migrate your current Orchestrator configuration, plug-ins, and data to the newly deployed Orchestrator Appliance manually.

After you upgrade the Orchestrator Appliance, your plug-in 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.

The following use case illustrates how to upgrade your existing Orchestrator Appliance by exporting its configuration and importing it to a newly deployed Orchestrator Appliance.

1 Verify that your Orchestrator Appliance is configured with an external database, certificates, licenses, and so on.

2 Export the Orchestrator configuration.

See "Export the Orchestrator Configuration," on page 91.

3 Deploy the latest Orchestrator Appliance.

See "Download and Deploy the Orchestrator Appliance," on page 25.

4 Import the configuration of your previous Orchestrator Appliance to the newly deployed Orchestrator Appliance.

See "Import the Orchestrator Configuration," on page 92.

5 Log in to the Orchestrator configuration interface of the newly deployed Orchestrator Appliance as **vmware**.

6 Update the database of the new Orchestrator Appliance.

See "Configure the Database Connection," on page 54.

7 Replace the IP address of the new Orchestrator Appliance with the IP address of your previous Orchestrator Appliance manually.

See "Configure the Network Connection," on page 39.

8 Restart the vRealize Orchestrator Configuration service.

9 Log in the Orchestrator client and verify that your workflows are available in the newly deployed Orchestrator Appliance.

Upgrade an Orchestrator Cluster

In the cluster, multiple Orchestrator server instances work together. If you have already set up a cluster of Orchestrator 5.5 server instances, you can upgrade the cluster to the latest Orchestrator version by upgrading its nodes.

Procedure

1 Stop all Orchestrator servers in the cluster.

2 Upgrade one of the Orchestrator server instances in the cluster.

3 Start the configuration service of the Orchestrator server you upgraded and log in to the configuration interface as **vmware**.

4 Click **Server Availability**.

5 Type values for the Cluster mode settings and click **Apply changes**.

Option	Description
Number of active nodes	The maximum number of active Orchestrator server instances in the cluster. Active nodes are the Orchestrator server instances that run workflows and respond to client requests. If an active Orchestrator node stops responding, it is replaced by one of the inactive Orchestrator server instances. The default number of active Orchestrator nodes in a cluster is one.
Heartbeat interval (milliseconds)	The time interval, in milliseconds, between two network heartbeats that an Orchestrator node sends to show that it is running. The default value is 5000 milliseconds.
Number of failover heartbeats	The number of heartbeats that can be missed before an Orchestrator node is considered failed. The default value is three heartbeats.

6 Upgrade all other Orchestrator server instances in the cluster.

7 Start all the Orchestrator nodes in the cluster.

Uninstall Orchestrator

You can remove the Orchestrator client and server components from your system by using **Add or Remove Programs**.

Prerequisites

- Save the Orchestrator configuration settings to a local file. For more details, see "Export the Orchestrator Configuration," on page 91.
- Back up custom workflows and plug-ins.

Procedure

1. From the Windows **Start** menu, select **Control Panel > Programs and Features**.
2. Select **vRealize Orchestrator** and click **Uninstall**.
3. Click **Uninstall** in the Uninstall vRealize Orchestrator window.

   A message confirms that all items have been successfully removed.
4. Click **Done**.

Orchestrator is uninstalled from your system.

Configuring vRealize Orchestrator 5

You can use the Orchestrator configuration interface 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 applications running on the Orchestrator platform.

The Orchestrator Web Configuration tool is installed with Orchestrator standalone. To use the tool, you must first start the Orchestrator Configuration Service.

To use Orchestrator, you must start the Orchestrator server service and then start the Orchestrator client.

To use Orchestrator through the vSphere Web Client, you must configure Orchestrator to work with the same vCenter Single Sign-On instance to which both vSphere Web Client and vCenter Server are pointing. You must also ensure that Orchestrator is registered as a vCenter Server extension. You register Orchestrator as a vCenter Server extension when you log in as a user who has the privileges to manage vCenter Server extensions. For more information, see "Configure the vCenter Server Plug-In," on page 62.

When you log in as an administrator, you can modify the configuration settings as required by your organization. For instructions about how to start the Orchestrator Server service, see "Start the Orchestrator Configuration Service," on page 38 and "Start the Orchestrator Server," on page 72. For more information about starting the Orchestrator client and using it, see *Using the VMware vRealize Orchestrator Client*.

When you install Orchestrator standalone, the Orchestrator server is also automatically configured to work, but you have to define a connection to a vCenter Server system if you plan to run workflows over the objects in your vSphere inventory. You can configure a connection to a vCenter Server system by running a workflow in the Orchestrator client. See *Using VMware vRealize Orchestrator Plug-Ins*.

The default Orchestrator database (embedded database) and LDAP (embedded LDAP) settings are not suitable for a production environment.

Preconfigured Software	User Group (if any) and User	Password
Embedded Database	User: vmware	vmware
Embedded LDAP	User group: vcoadmins User: vcoadmin By default the vcoadmin user is set up as an Orchestrator administrator.	vcoadmin

To use Orchestrator in a production deployment, you must set up a separate database instance, set up an LDAP or vCenter Single Sign-On server, and configure Orchestrator to work with them.

NOTE LDAP authentication is deprecated.

To configure the Orchestrator server, you can run configuration workflows by using the Orchestrator client or the REST API. For information about configuring Orchestrator by using the Configuration plug-in workflows, see *Using VMware vRealize OrchestratorPlug-Ins*. For more information about configuring Orchestrator by using the REST API, see Chapter 7, "Configuring Orchestrator by Using the Configuration Plug-In and the REST API," on page 79.

IMPORTANT When you configure Orchestrator, ensure that the clocks of the Orchestrator server machine and the Orchestrator client machine are synchronized.

This chapter includes the following topics:

Start the Orchestrator Configuration Service

If you have installed Orchestrator standalone, the Orchestrator Configuration service does not start by default. You must start it manually before you try to access the Orchestrator configuration interface.

Procedure

1 On the machine on which Orchestrator is installed, select **Start > Programs > Administrative Tools > Services**.

2 In the Services window, right-click **VMware vRealize Orchestrator Configuration** and select **Start**.

3 (Optional) Set up the service to start automatically on the next reboot.

   a Right-click **VMware vRealize Orchestrator Configuration** and select **Properties**.

   b In the VMware vRealize Orchestrator Configuration Properties (Local Computer) window, from the **Startup type** drop-down menu select **Automatic**.

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

Verify that the VMware vRealize Orchestrator Configuration service is running.

Procedure

1 Start the Orchestrator configuration interface.

- If you are logged in to the Orchestrator server machine as the user who installed Orchestrator, select **Start > Programs > VMware > vRealize Orchestrator Home Page**, and click **Orchestrator Configuration**.
- Go to https://localhost:8281 in a Web browser and click **Orchestrator Configuration**.
- If you want to connect to the Orchestrator configuration from a remote computer, navigate to https://*your_orchestrator_server_IP_or_DNS_name*:8283/vco-config.

  You can log in to the Orchestrator configuration interface remotely only over HTTPS.

2 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.

3 Change the default password and click **Apply changes**.

IMPORTANT Your new password must be at least eight characters long, and must contain at least one digit, special character, and uppercase letter.

The next time you log in to the Orchestrator configuration interface, you can use your new password.

IMPORTANT The password for the root account of the Orchestrator Appliance expires after 365 days. You can increase the expiry time for an account by logging in to the Orchestrator Appliance as root, and running `passwd –x number_of_days name_of_account`. If you want to increase the Orchestrator Appliance root password to infinity, run `passwd –x 99999 root`.

You successfully logged in to the Orchestrator configuration interface.

Configure the Network Connection

To change the IP address that the Orchestrator client interface uses to communicate to the server, 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 40.

5 Click **Apply changes**.

What to do next

Click **SSL Trust Manager** to load the vCenter Server SSL certificate in Orchestrator.

Orchestrator Network Ports

Orchestrator uses specific ports that allow communication with the other systems. 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 firewalls as required.

Default Configuration Ports

To provide the Orchestrator service, you must set 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 5-1. VMware vRealize Orchestrator Default Configuration Ports

Port	Number	Protocol	Source	Target	Description
HTTP server port	8280	TCP	End-user Web browser	Orchestrator server	The requests sent to Orchestrator default HTTP Web port 8280 are redirected to the default HTTPS Web port 8281.
HTTPS server port	8281	TCP	End-user Web browser	Orchestrator server	The access port for the Web Orchestrator home page.
Web configuration HTTPS access port	8283	TCP	End-user Web browser	Orchestrator configuration	The SSL access port for the Web UI of Orchestrator configuration.
Messaging port	8286	TCP	Orchestrator client	Orchestrator server	A Java messaging port used for dispatching events.
Messaging port	8287	TCP	Orchestrator client	Orchestrator server	An SSL secured Java messaging port used for dispatching events.

External Communication Ports

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

Table 5-2. VMware vRealize Orchestrator External Communication Ports

Port	Number	Protocol	Source	Target	Description
LDAP	389	TCP	Orchestrator server	LDAP server	The lookup port of your LDAP Authentication server. **NOTE** LDAP authentication is deprecated.
LDAP using SSL	636	TCP	Orchestrator server	LDAP server	The lookup port of your secure LDAP Authentication server.
LDAP using Global Catalog	3268	TCP	Orchestrator server	Global Catalog server	The port to which Microsoft Global Catalog server queries are directed.
vCenter Single Sign-On server	7444	TCP	Orchestrator server	vCenter Single Sign-On server	The port used to communicate with the vCenter Single Sign-On server.
SQL Server	1433	TCP	Orchestrator server	Microsoft SQL Server	The port used to communicate with the Microsoft SQL Server or SQL Server Express instances that are configured as the Orchestrator database.
PostgreSQL	5432	TCP	Orchestrator server	PostgreSQL Server	The port used to communicate with the PostgreSQL Server that is configured as the Orchestrator database.
Oracle	1521	TCP	Orchestrator server	Oracle DB Server	The port used to communicate with the Oracle Database Server that is configured as the Orchestrator database.
SMTP Server port	25	TCP	Orchestrator server	SMTP Server	The port used for email notifications.
vCenter Server API port	443	TCP	Orchestrator server	vCenter Server	The vCenter Server API communication port used by Orchestrator to obtain virtual infrastructure and virtual machine information from the orchestrated 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.

NOTE LDAP authentication is deprecated.

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.

Option	Action
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\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.

Selecting the Authentication Type

Orchestrator requires an authentication method to work properly and manage user permissions.

Orchestrator supports the following types of authentication.

LDAP authentication Orchestrator connects to a working LDAP server.

NOTE LDAP authentication is deprecated.

vCenter Single Sign-On authentication Orchestrator authenticates through vCenter Single Sign-On.

vRealize Automation authentication Orchestrator authenticates through the vRealize Automation component registry.

Depending on the type of installation, Orchestrator is preconfigured to work with either an embedded LDAP server or OpenLDAP.

- When you install Orchestrator standalone, the Orchestrator server is preconfigured to work with an embedded LDAP server.
- When you download and deploy the Orchestrator Appliance, the Orchestrator server is preconfigured to work with the OpenLDAP directory service embedded in the appliance.

IMPORTANT If you want to use Orchestrator through the vSphere Web Client for managing vSphere inventory objects, you must configure Orchestrator to work with the same vCenter Single Sign-On instance to which both vCenter Server and vSphere Web Client are pointing.

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 and later, users authenticate by using vCenter Single Sign-On.

For versions earlier than vCenter Server 5.1, you must explicitly register each vCenter Server system with the vSphere Web Client. For vCenter Server 5.1 and later, vCenter Server systems are automatically detected and are displayed in the vSphere Web Client inventory.

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. You must provide 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 providing 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.

Option	Action
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 vRO 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`

NOTE If you want to configure Orchestrator to authenticate through the vCenter Single Sign-On in the vCenter Server Appliance, you must set the port to 443.

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 an Orchestrator administrator 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/vsphere.local

   NOTE If you want to configure Orchestrator to authenticate through the vCenter Single Sign-On in the vCenter Server Appliance, you must set the port to 443.

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/vsphere.local

   NOTE If you want to configure Orchestrator to authenticate through the vCenter Single Sign-On in the vCenter Server Appliance, you must set the port to 443.

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 an Orchestrator administrator 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

You can configure Orchestrator to connect to a working LDAP server on your infrastructure to manage user permissions.

NOTE LDAP authentication is deprecated.

If you are using secure LDAP over SSL, Windows Server 2008 or 2012, and AD, verify that the **LDAP Server Signing Requirements** group policy is disabled on the LDAP server.

If you configure Orchestrator to work with LDAP, you cannot use the Orchestrator Web Client for managing vSphere inventory objects.

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.

1 Import the LDAP Server SSL Certificate on page 47

   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.

2 Generate the LDAP Connection URL on page 47

   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.

3 Specify the Browsing Credentials on page 49

   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 50

   You can define the users and groups lookup information.

5 Define the LDAP Search Options on page 51

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

6 Common Active Directory LDAP Errors on page 52

   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.

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 2008 or 2012, 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.

Option	Action
Import from URL	Type the URL of the LDAP server: **`https://`*`your_LDAP_server_IP_address`*** or ***`your_LDAP_server_IP_address:port`***
Import from file	Obtain the LDAP SSL certificate file and browse to import it.

6 Click **Import**.

A message confirming that the import is successful appears.

7 Click **Startup Options**.

8 Click **Restart the vRO 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, OpenLDAP, 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 47.

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 49.

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 **vRO 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 **vRO 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 vRO 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 **Authentication**.

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

4 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.

5 (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.

6 (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.

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

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

8 In the **Host reachable timeout** text box, type a value in milliseconds.

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

9 Click **Apply changes**.

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

What to do next

Configure the database. For more information, see "Configuring the Orchestrator Database Connection," on page 52.

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 5-3. Common Active Directory Authentication Errors

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

Configuring the Orchestrator Database Connection

The Orchestrator server requires a database for storing data.

The type of Orchestrator installation determines the kind of database it works with.

- When you install Orchestrator standalone, the Orchestrator server is preconfigured to work with an embedded database.
- When you download and deploy the Orchestrator Appliance, the Orchestrator server is preconfigured to work with the PostgreSQL database embedded in the appliance.

The embedded and PostgreSQL databases are suitable only for small-scale, medium-scale, and testing environments. If you decide to use an embedded database, you cannot set up Orchestrator to work in cluster mode, or change any licenses and the server certificate by using the Orchestrator configuration interface. To change the license key and the server certificate without changing the database, you must run the configuration workflows by using either the Orchestrator client or the REST API. For more information about running the configuration workflows by using the Orchestrator client, see *Using the VMware vRealize Orchestrator Plug-Ins*. For instructions about running the configuration workflows by using the REST API, see Chapter 7, "Configuring Orchestrator by Using the Configuration Plug-In and the REST API," on page 79.

For better performance in a production environment, install a relational database management system (RDBMS) and create a new database for Orchestrator. For more information about creating a new database for Orchestrator, see "Setting Up the Orchestrator Database," on page 20. If you decide to use a separate database, configure the database for remote connection. For an example of configuring SQL Server Express for remote connection, see "Configure SQL Server Express to Use with Orchestrator," on page 52.

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.

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.

Option	Action
Import from URL	Type the URL of the database server: `https://your_database_server_IP_address` or `your_database_server_IP_address:port`
Import from file	Obtain the database 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 vRO 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 the Orchestrator database, you must set the database connection parameters.

Prerequisites

- Set up a new database to use with the Orchestrator server. See "Setting Up the Orchestrator Database," on page 20.
- If you are using an SQL Server database configured to use dynamic ports, verify that the SQL Server Browser service is running.
- To prevent possible transactional deadlocks when the database is Microsoft SQL Server database, set the `ALLOW_SNAPSHOT_ISOLATION` and `READ_COMMITTED_SNAPSHOT` database options on.
- To avoid an `ORA-01450` error when using the Oracle database, verify that you have configured the database block size properly. The minimum allowed size depends on the block size your Oracle database index is using.
- 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 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 53.

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.

Option	Description
Oracle	Configures Orchestrator to work with an Oracle database instance.
SQL Server	Configures Orchestrator to work with a Microsoft SQL Server or Microsoft SQL Server Express database instance.
PostgreSQL	Configures Orchestrator to work with a PostgreSQL database instance.
vDB	Configures Orchestrator to work with the vCenter Server database.
Embedded Database	Configures Orchestrator to work with the embedded database.

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

Option	Description
User name	The user name that Orchestrator uses to connect and operate the selected database. The name you select must be a valid user on the target database with **db_owner** rights. This option is applicable for all databases.
Password (if any)	The password for the user name. This option is applicable for all databases.
Use SSL	Select to use an 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.
Database server IP address or DNS name	The database server IP address or DNS name. This option is applicable for all databases.
Port	The database server port is used for communication to your database. This option is applicable for all databases.
Database name	The full unique name of your database. The database name is specified in the `SERVICE_NAMES` parameter in the initialization parameter file. This option is valid only for SQL Server, and PostgreSQL databases.
Instance name (if any)	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.
Domain	To use Windows authentication, type the domain name of the SQL Server machine, for example company.org. To use SQL authentication, leave this text box blank. This option is valid only for SQL Server and specifies whether you want to use Windows or SQL Server authentication.
Use Windows authentication mode (NTLMv2)	Select to send NTLMv2 responses when using Windows authentication. This option is valid only for SQL Server.

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.

Option	Description
Create the database tables	Builds a new table structure for the Orchestrator database.
Update the database	Uses the database from your previous Orchestrator installation and updates the table structure.

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

Example: Configure Orchestrator to Work with SQL Server Express by Using Windows Authentication Mode

If you want to use Orchestrator in small scale deployments for testing purposes, you might want to use SQL Server Express 2008. After you create a new database, for example *Orchestrator*, and enable it for remote connection, perform the following steps to configure the database connection:

1 Log in to the Orchestrator configuration interface as vmware.

2 Click the **Database** tab.

3 From the **Select the database type** drop-down menu, select **SQLServer**.

4 In the **User name** and **Password (if any)** text boxes, type your Windows credentials.

5 In the **Database server IP address or DNS name** text box, type the IP address of the machine on which Orchestrator and the database are installed.

6 In the **Port** text box, type the TCP/IP port of SQL Server, which usually is `1433`.

7 In the **Database name** text box, type the name of the SQL Server Express database you created, for example `Orchestrator`.

8 In the **Instance name (if any)** text box, type the name of the database instance.

   You can leave this field blank if you have only one instance of SQL Server installed on the machine.

9 In the **Domain** text box, either type the domain name of the machine on which Orchestrator and the database are installed, or type `localhost`.

10 Select **Use Windows authentication mode (NTLMv2)**.

11 Click **Apply**.

12 Build or update the database as necessary and click **Apply changes**.

You successfully configured Orchestrator to work with SQL Server Express by using Windows authentication mode.

Server Certificate

The Package Signing Certificate is a form of digital identification that is used to guarantee encrypted communication and a signature for your Orchestrator packages.

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 a package, the client verifies your identity and decides whether to trust your signature.

Important You cannot change the server certificate by using the Orchestrator configuration interface if Orchestrator uses an embedded database. To change the server certificates without changing the database settings, you must run the configuration workflows by using either the Orchestrator client or the REST API. For more information about running the configuration workflows by using the Orchestrator client, see *Using the VMware vRealize Orchestrator Plug-Ins*. For detailed instructions about running the configuration workflows by using the REST API, see Chapter 7, "Configuring Orchestrator by Using the Configuration Plug-In and the REST API," on page 79.

- Create a Self-Signed Server Certificate on page 57

  Deploying the Orchestrator Appliance requires that you create a 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 that you are sending is in fact a package issued by your server and not a third party claiming to be you.

- Obtain a Server Certificate Signed by a Certificate Authority on page 57

  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.

- Import a Server Certificate on page 58

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

- Export a Server Certificate on page 58

  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 contents of the exported packages signed with this certificate become unavailable. To ensure that packages are decrypted on import, you must save this key to a local file.

- Changing a Self-Signed Server Certificate on page 59

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

Create a Self-Signed Server Certificate

Deploying the Orchestrator Appliance requires that you create a 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 that 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 Type 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's public key appear in the Server Certificate window. The certificate's 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.

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 `VS0certificate.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.

   The CA returns a certificate that you must import.

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

Orchestrator uses the server certificate to perform the following tasks:

- Signs all packages before they are exported by attaching your certificate's public key to each one.
- Displays a user prompt after users import a package that contains elements signed by untrusted certificates.

What to do next

You can import this certificate on other servers.

Import a Server Certificate

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

IMPORTANT You can import a certificate only if you have not created a self-signed certificate. If you have already created a certificate in the database, the option to import a certificate is not available.

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 Type the password used to decrypt the content of the imported keystore database.

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

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 contents of the exported packages signed with this certificate 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 Type 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.

Changing 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 must export all your packages and change the Orchestrator database.

This workflow describes the process to change the Orchestrator self-signed certificate.

1 Export all your packages by using the Orchestrator client.

a Select **Administer** from the drop-down menu in the left upper corner of the Orchestrator client.

b Click the **Packages** view.

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

d Browse to select a location to save the package to and click **Save**.

e Leave the **View content**, **Add to package**, and **Edit contents** options selected.

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

f (Optional) Deselect the **Export the values of the configuration settings** check box if you do not want to export the values of the configuration elements attributes in the package.

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

h Click **Save**.

2 Create a new database and configure Orchestrator to work with it.

You configure the Orchestrator database connection by using the Orchestrator configuration interface. For more information about setting up the Orchestrator database, see "Configure the Database Connection," on page 54.

3 (Optional) Export the Orchestrator configuration to back up your configuration data in case you want to use the old database and the old SSL certificate.

You can export the Orchestrator configuration by using the Orchestrator configuration interface. For more information, see "Export the Orchestrator Configuration," on page 91.

4 (Optional) Back up your database if you want to retain the old data.

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

5 Create a new self-signed certificate or import a server certificate signed by a certification authority.

You can create and import self-signed certificates by using the Orchestrator configuration interface. For more information, see "Server Certificate," on page 56.

6 Import your license keys.

You can configure the license settings from the Orchestrator configuration interface. For more information, see "Import the vCenter Server License," on page 63.

7 Reinstall the default Orchestrator plug-ins.

a On the Orchestrator configuration interface, click the **Troubleshooting** tab.

b Click the **Reset current version** link.

8 Restart the Orchestrator server.

a On the Orchestrator configuration interface, click the **Startup options** tab.

b Click the **Restart service** link.

9 Reimport your packages.

a Select **Administer** from the drop-down menu in the left upper corner of the Orchestrator client.

b Click the **Packages** view.

c Right-click under the available packages, and from the pop-up menu, select **Import package**.

d Browse to the package to import and click **Open**.

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

f (Optional) Deselect the **Import the values of the configuration settings** check box if you do not want to import the values of the configuration elements attributes from the package.

g Click **Import checked elements**.

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

Configure the Orchestrator Plug-Ins

To deploy the standard set of plug-ins when the Orchestrator server starts, the Orchestrator system must authenticate against an LDAP or vCenter Single Sign-On server. You first specify the administrative credentials that Orchestrator uses with the plug-ins, and enable or disable plug-ins.

If you change the Orchestrator database after configuring and installing the plug-ins, you must click the **Reset current version** link on the **Troubleshooting** tab. This operation deletes the *`install_directory`*`\app-server\conf\plugins\_VSOPluginInstallationVersion.xml` file, which contains information about the version of the plug-ins already installed, and forces plug-in reinstallation.

Prerequisites

Set up an LDAP or vCenter Single Sign-On server and configure the Orchestrator authentication settings.

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 administrators group that you specified on the **Authentication** 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) To disable a plug-in, deselect the check box next to it.

This action does not remove the plug-in file.

5 Click **Apply changes**.

The first time the server starts, it installs the selected plug-ins.

What to do next

You can configure the settings for Mail and SSH plug-ins.

Define the Default SMTP Connection

The Mail plug-in is installed together with the 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 might receive `SMTP_HOST_UNREACHABLE` error.

Procedure

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

2 Click **Mail**.

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

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

4 Click **Apply changes**.

Configure the SSH Plug-In

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

Procedure

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

2 Click **SSH**.

3 Click **New connection**.

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

NOTE No username and password are 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 client.

Configure the vCenter Server Plug-In

You can configure Orchestrator to connect to your vCenter Server instances by running the vCenter workflows in the Orchestrator client.

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 same vCenter Single Sign-On instance to which both vCenter Server and vSphere Web Client are pointing. You must also ensure that Orchestrator is registered as a vCenter Server extension. You register Orchestrator as a vCenter Server extension when you specify a user (by providing the user name and password), who has the privileges to manage vCenter Server extensions.

What to do next

Import the SSL certificates for each vCenter Server instance that you defined.

Installing a New Plug-In

After you configure the default Orchestrator plug-ins, you might want to install a new plug-in.

All Orchestrator plug-ins are installed from the Orchestrator configuration interface. 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.

You install `.vmoapp` files from the **General** tab of the Orchestrator configuration interface, and `.dar` files from the **Plug-ins** tab.

Install a New Plug-In Distributed as a DAR File

After you configure the default Orchestrator plug-ins you might want to install a new `.dar` plug-in.

Procedure

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

2 Click the **Plug-ins** tab.

3 Click the magnifying glass icon under Install new plug-in.

4 Browse to locate the `.dar` file, and click **Open**.

5 Click **Upload and install**.

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

Install a New Plug-In Distributed as a VMOAPP File

After you configure the default Orchestrator plug-ins, you might want to install a new `.vmoapp` plug-in.

Procedure

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

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

3 Click the magnifying glass icon.

4 Browse to locate the `.vmoapp` file, and click **Open**.

5 Click **Install**.

The tab for the plug-in appears in the Orchestrator configuration interface.

6 On the **Startup Options** tab, click **Restart service** to complete the plug-in installation.

You successfully installed the plug-in. Every time you install a `.vmoapp` plug-in, 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.

Importing the vCenter Server License

To complete the configuration process for the Orchestrator server, you must import the vCenter Server license. The set of plug-ins delivered with Orchestrator does not require a license. If you add a plug-in that requires a license, you must import the license.

The procedure for installing plug-in licenses is the same as that for adding a vCenter Server license manually.

You cannot import a license key from the Orchestrator configuration interface if Orchestrator uses embedded database. To import the license without changing the database, run the respective configuration workflows by using either the Orchestrator client or the REST API. For more information about running the configuration workflows by using the Orchestrator client, see *Using the VMware vRealize OrchestratorPlug-Ins*. For information about running the configuration workflows by using the REST API, see Chapter 7, "Configuring Orchestrator by Using the Configuration Plug-In and the REST API," on page 79.

Import the vCenter Server License

If the version of your vCenter Server is later than version 4.0, you must import the vCenter Server license.

Prerequisites

- Verify that the Orchestrator database is not embedded. Otherwise, the **Licenses** tab is dimmed.
- Import the SSL certificate for the licensed vCenter Server host. See "Import the vCenter Server SSL Certificate," on page 41.

Procedure

1. Log in to the Orchestrator configuration interface as **`vmware`**.
2. Click **Licenses**.
3. On the **vCenter Server License** tab, provide 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 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, preferably at the top of the vSphere tree structure.
4. (Optional) To view details of the license to import, click **License details**.
5. Click **Apply changes**.
6. (Optional) To view the license details, click the name of the imported license.
7. Start the Orchestrator server.

The Orchestrator server is now configured correctly.

Add the vCenter Server License Key Manually

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

Prerequisites

- Verify that the Orchestrator database is not embedded. Otherwise, the **Licenses** tab is dimmed.
- Import the SSL certificate for the licensed vCenter Server host. See "Import the vCenter Server SSL Certificate," on page 41.

Procedure

1. Log in to the Orchestrator configuration interface as **vmware**.
2. Click **Licenses**.
3. On the **vCenter Server License** tab, select **Add vCenter Server license manually**.
4. In the **Serial number** text box, type your vCenter Server license key.
5. In the **License owner** text box, type a name for the owner of the license.
6. Click **Apply changes**.
7. Start the Orchestrator server.

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 5-4. Orchestrator Server Modes

vCenter Server License Edition	vRealize Orchestrator Mode	Description
Standard	Server	You are granted full read and write privileges to all Orchestrator elements. You can run and edit workflows.
Foundation	Player	You are granted read privileges on all Orchestrator elements. You can run workflows but you cannot edit them.
Essentials	Player	You are granted read privileges on all Orchestrator elements. You can run workflows but you cannot edit them.
Evaluation	Server	You are granted full read and write privileges to all Orchestrator elements. You can run and edit workflows.

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.

Selecting the Orchestrator Server Mode

By default, the Orchestrator server runs as a single instance in standalone mode. To increase the availability of the Orchestrator services, you can set up the Orchestrator server to work in cluster mode and start multiple Orchestrator server instances in a cluster with a shared database.

Orchestrator supports two server modes.

Standalone mode The Orchestrator server runs as a standalone instance.

Cluster mode Multiple Orchestrator server instances with identical server and plug-ins' configurations work together in a cluster and share one database. Only the active Orchestrator server instances respond to client requests and run workflows.

All Orchestrator server instances communicate with each other by exchanging heartbeats. Each heartbeat is a timestamp that the node writes to the cluster shared database at a certain time interval. Network problems, an unresponsive database server, or overloading might cause an Orchestrator cluster node to stop responding. If an active Orchestrator server instance fails to send heartbeats for the failover timeout, it is considered as non-responsive. The failover timeout is equal to the value of the heartbeat interval multiplied by the number of the failover heartbeats. It serves as a definition for an unreliable node and must be customized according to the available resources and the production load.

The non-responsive node is automatically shut down and one of the inactive instances takes control to resume all interrupted workflows from their last not completed items, such as scriptable tasks, workflow invocations, and so on. You can restart the node that was shut down by using an external script based on the Orchestrator REST API or manually.

Orchestrator does not provide a built-in tool for monitoring the cluster status and sending notifications in case of a failover. You can monitor the cluster state by using an external component such as a load balancer. To identify if a node is running, you can check if the REST API of this node is responding properly.

IMPORTANT In cluster mode, when more than one Orchestrator server is active, the use of the Orchestrator client is not supported. If you have more than one active Orchestrator node in a cluster, when different users use the different Orchestrator nodes to modify one and the same resource, concurrency problems occur. To have more than one active Orchestrator server node in a cluster, you must develop the workflows that you need when Orchestrator is in standalone mode, and after that set up Orchestrator to work in cluster mode.

Configure Cluster Mode

To increase the availability of Orchestrator services, you can configure a cluster of Orchestrator server instances.

An Orchestrator cluster consists of at least two Orchestrator server instances that share one database.

IMPORTANT To work properly in the cluster, all Orchestrator server instances must be configured identically with each other and must have the same plug-ins installed. After you set up the Orchestrator cluster, do not change the configurations of its nodes.

Prerequisites

- Configure the database that you plan to use as a shared database to accept multiple connections, so that it can accept connections from the different Orchestrator instances.

  To prevent possible transactional deadlocks when the database is Microsoft SQL Server database, you must set the `ALLOW_SNAPSHOT_ISOLATION` and `READ_COMMITTED_SNAPSHOT` database options on.

- Install and configure at least two identical Orchestrator server instances.

  If you export the configuration of one Orchestrator server instance and import it to another Orchestrator server or if you clone the machine on which the Orchestrator server is running, you must type the credentials for the new Orchestrator server that you want to use to establish the connection to your vCenter Server instance. You can do this on the **vCenter Server** tab of the Orchestrator configuration interface.

- Verify that the Orchestrator instances use the same database.
- Synchronize the clocks of the machines on which the Orchestrator server instances are installed.

Procedure

1 Log in to the Orchestrator configuration interface of the first Orchestrator server as **`vmware`**.

2 Click **Server Availability**.

3 Select the **Cluster mode** check box.

  If you have configured the Orchestrator server nodes properly, Orchestrator detects the other nodes when you select the check box.

4 (Optional) Provide values for the Cluster mode settings and click **Apply changes**.

Option	Description
Number of active nodes	The maximum number of active Orchestrator server instances in the cluster. Active nodes are the Orchestrator server instances that run workflows and respond to client requests. If an active Orchestrator node stops responding, it is replaced by one of the inactive Orchestrator server instances. The default number of active Orchestrator nodes in a cluster is one.
Heartbeat interval (milliseconds)	The time interval, in milliseconds, between two network heartbeats that an Orchestrator node sends to show that it is running. The default value is 5000 milliseconds.
Number of failover heartbeats	The number of heartbeats that can be missed before an Orchestrator node is considered failed. The default value is 12 heartbeats.

  The default failover timeout is 1 minute and is equal to the value of the default heartbeat interval multiplied by the number of the default failover heartbeats.

5 Log in to the Orchestrator configuration interface of the second Orchestrator server as **`vmware`**.

6 Repeat Step 3 and Step 4.

You have set up an Orchestrator cluster.

What to do next

You can add more Orchestrator cluster nodes.

Important When you configure Orchestrator to work in cluster mode, you must first start one of the Orchestrator servers and wait until it starts and initializes the database. A cluster node is considered running when on the **Server Availability** tab, the node appears under Started cluster nodes with a Running status. If you start more than one Orchestrator servers at the same time, concurrency issues occur as all of the started Orchestrator servers try to initialize the database.

Configuring a Cluster of Orchestrator Server Instances

To increase the availability of Orchestrator, you can configure a cluster of Orchestrator server instances. In the cluster, multiple Orchestrator server instances (Orchestrator server nodes) work together. To achieve this, the nodes must share one database and have identical configuration of the Orchestrator server and plug-ins.

The active Orchestrator server nodes respond to client requests and run workflows. If an active Orchestrator server node fails to send heartbeats to indicate it is up and running, it is considered as non-responsive and an inactive Orchestrator node becomes active to take control and resume all of the workflows from the point they were interrupted.

After you configure an Orchestrator server instance in cluster mode, you can create the rest of the Orchestrator cluster nodes by exporting the configuration of the main Orchestrator server instance and importing it to the newly installed Orchestrator server instances.

Note All Orchestrator server nodes of a cluster must have identical server and plug-ins' configuration and contents. If you want to make changes on the Orchestrator content, for example to edit a workflow or an action, you must stop all Orchestrator server nodes except one and cancel all running tasks that refer to the content you want to change. You can then make changes to the only server node that is active, and restart the other Orchestrator server instances in the cluster.

The following use case describes how to build an Orchestrator cluster by installing and configuring the main Orchestrator server instance (Orchestrator server 1) and importing its configuration to a newly installed Orchestrator server instance (Orchestrator server 2).

1 Install Orchestrator server 1 or download and deploy the Orchestrator Appliance.

   For information about installing Orchestrator standalone, see "Install Orchestrator Standalone," on page 23. For information about downloading and deploying the Orchestrator Appliance, see "Download and Deploy the Orchestrator Appliance," on page 25.

2 Configure a database instance.

   Important Configure the database to accept multiple connections so that it can accept connections from the different Orchestrator instances. To prevent possible transactional deadlocks when the database is Microsoft SQL Server database, you must set the `ALLOW_SNAPSHOT_ISOLATION` and `READ_COMMITTED_SNAPSHOT` database options to on.

   You must use an external database.

3 Log in to the Orchestrator configuration interface as **`vmware`**, and configure Orchestrator server 1 to work with the database you configured.

   See "Configuring the Orchestrator Database Connection," on page 52.

4 Configure Licensing.

   See "Importing the vCenter Server License," on page 63

5 Click the **Reset current version** link on the **Troubleshooting** tab to reinstall previously installed Orchestrator plug-ins with the newly configured database.

   See "Configure the Orchestrator Plug-Ins," on page 60.

6 Configure an authentication provider.

   See "Selecting the Authentication Type," on page 42.

7 Configure Orchestrator server 1 to work in cluster mode.

   See "Configure Cluster Mode," on page 65.

8 (Optional) Install and configure additional Orchestrator plug-ins.

   See "Installing a New Plug-In," on page 62

9 Start Orchestrator server 1 and wait until it starts successfully.

10 Restart the configuration interface and export the Orchestrator server 1 configuration.

   See "Export the Orchestrator Configuration," on page 91.

11 Install Orchestrator server 2 or download and deploy the Orchestrator Appliance.

   For information about installing Orchestrator standalone, see "Install Orchestrator Standalone," on page 23. For information about downloading and deploying the Orchestrator Appliance, see "Download and Deploy the Orchestrator Appliance," on page 25.

12 On Orchestrator server 2, install the plug-ins that you have installed on Orchestrator server 1.

13 Import the Orchestrator configuration of Orchestrator server 1 to Orchestrator server 2.

   By importing the Orchestrator configuration, you make both configurations identical. For more information about importing the Orchestrator configuration, see "Import the Orchestrator Configuration," on page 92.

14 Verify that both Orchestrator server instances have identical configurations and configure the plug-ins on Orchestrator server 2 identically with the plug-ins on Orchestrator server 1.

15 Modify the network settings on both Orchestrator server instances to reflect your environment, if necessary.

   For instructions about configuring the Orchestrator network settings, see "Configure the Network Connection," on page 39.

16 Synchronize the the clock of the Orchestrator server 2 machine with the clock of the Orchestrator server 1 machine.

17 Start Orchestrator server 2.

   To verify that the server started successfully, click the **Server Availability** tab of the Orchestrator configuration interface and wait until the name of the Orchestrator server appears under Started cluster nodes with a Running or StandBy status.

You can add more Orchestrator server active nodes to the cluster by changing the value of the **Number of active nodes** field in the **Server Availability** tab.

Configuring a Load Balancer

Load balancers distribute work among servers in high-availability deployments.

After you configure the Orchestrator server mode, you can set up a load balancer to distribute traffic among multiple instances of vRealize Orchestrator. For specific information on configuring the F5 and NSX load balancers, see "Configure the F5 Load Balancer to Work With an Orchestrator Cluster," on page 70 and "Configure the NSX Load Balancer to Work With an Orchestrator Cluster," on page 69

Configure the NSX Load Balancer to Work With an Orchestrator Cluster

To increase the availability of the VMware vRealize Orchestrator services both in standalone and cluster mode, you can put the Orchestrator behind a load balancer.

Prerequisites

Configure at least two Orchestrator nodes.

Procedure

1 Create and configure the NSX-Edge.

   a Log in to the vCenter Server where NSX has been configured.

   b Navigate to **Home > Networking & Security > NSX Edges** and create your own NSX edge.

   c Navigate to **Manage > Settings > Interfaces**.

   d Select the first vNIC and click the **Edit** button.

   This is your load balancer virtual appliance.

   e Click the **Add** button to assign a static IP address to the virtual interface.

2 Configure Application Profiles.

   a Log in to the vCenter Server where NSX has been configured.

   b Navigate to **Home > Networking & Security > NSX Edges** and create your own NSX edge.

   c On the **Load Balancer** tab select the **Application Profiles** menu.

   d Click the **Add** button to create a new profile and complete the form according to the table below:

Name	Type	Enabled SSL Pass-through	Persistence	Client Authentication
vROProfile	HTTPS	yes	None	Ignore

   e Click **OK**.

3 Configure Service Monitoring.

   a Log in to the vCenter Server where NSX has been configured.

   b Navigate to **Home > Networking & Security > NSX Edges** and create your own NSX edge.

   c On the **Load Balancer** tab select the **Service Monitoring** menu.

   d Click the **Add** button to create a new monitor and complete the form according to the table below:

Monitor	Interval	Timeout	Max Retries	Type	Method	URL	Receive
vro-https-8281	3	9	3	HTTPS	GET	/vco/api/docs/index.html HTTP/1.1\r\nHost:\r\n\nConnection: close\r\n\r\n	200 OK

4 Configure Pools.

   a Log in to vCenter Server where NSX has been set up.

   b Navigate to **Home > Networking & Security > NSX Edges** and create your own NSX edge.

   c On the **Load Balancer** tab select **Pools**.

d Click on the **Add** button to create a new pool and complete the form according to the table below:

Name	Algorithm	Monitors
vro-pool	Round Robin	vro-https-8281

e Click on the **Add** button to add members:

Enabled Member	Name	IP Address / VC Container	Monitor Port	Port
yes	HA-cluster-vro1	vro-Node1-IP	8281	8281
yes	HA-cluster-vro2	vro-Node2-IP	8281	8281

The green status indicates that the node is active.

f Click on **Show Pool Statistics** and verify that the pool is in **UP** state.

5 Configure Virtual Servers.

a Log in to vCenter Server where NSX has been set up.

b Navigate to **Home > Networking & Security > NSX Edges** and create your own NSX edge.

c On the **Load Balancer** tab select **Virtual Servers**.

d Click on the **Add** button to create a new virtual server and complete the form according to the table below:

Enable VS	Application Profile	Name	IP Address	Protocol	Port	Default Pool
yes	vROProfile	vro-lb-8281	vro-lb-IP	HTTPS	8281	vro-pool

NOTE The port number of the virtual server must correspond to the port number of the pool.

You have successfully configured the NSX load balancer to work with a vRealize Orchestrator cluster.

Configure the F5 Load Balancer to Work With an Orchestrator Cluster

To increase the availability of the VMware vRealize Orchestrator services both in standalone and cluster mode, you can put the Orchestrator behind a load balancer.

Prerequisites

Configure at least two Orchestrator nodes.

Procedure

1 Configure monitors.

a Log in to the F5 load balancer and select **Local Traffic > Monitors** from the main menu.

b Create a monitor named **`vco-https-8281`** and configure the settings as follows:

Monitor	Interval	Timeout	Retries	Type	Send String	Recieve String	Alias Service Port
vco-https-8281	3	9	3	HTTPS (443)	GET /vco/api/docs/index.html HTTP/1.1\r\nHost:\r\n\nConnection: close\r\n\r\n	200 OK	8281

Leave all other fields with their default values.

c Click **Finished**.

2 Configure server pools.

a Navigate to **Local Traffic > Pools** from the main menu.

b Create a pool named **`vro-pool-8281`** and configure the settings as follows:

Pool Name	LB Method	Health Monitors
vro-pool-8281	Round Robin	vro-https-8281

Leave all other fields with their default values.

c Add two new nodes in the **New Members** section:

Name	Address	Service Port
vro-node1-hostname.domain.com	vro-node1-IP	8281
vro-node2-hostname.domain.com	vro-node2-IP	8281

d Click **Finished**.

Pool Name	LB Method	Health Monitors	Node Name	Address	Service Port
vro-pool-8281	Round Robin	vro-https-8281	vro-node1-hostname.domain.com	vro-node1-IP	8281
vro-pool-8281	Round Robin	vro-https-8281	vro-node2-hostname.domain.com	vro-node2-IP	8281

The green status indicates that the node is active.

3 Configure virtual servers.

a Navigate to **Local Traffic > Virtual Servers** from the main menu.

b Create a virtual server named **`vro-lb-8281`** and configure the settings as follows:

Name	Type	Destination Address	Service Port	Source Address Translation	Default Pool Name
vco-lb-8281	Performance (Layer 4)	vro-lb-IP	8281	Automap	vro-pool-8281

Leave all other fields with their default values.

4 Verify that the high-availability environment is correctly configured.

a Navigate to **Local Traffic > Network Map** from the main menu.

b Verify that all entries on the network map are listed as green.

You have successfully configured the F5 load balancer to work with a vRealize Orchestrator cluster.

Configure Orchestrator to Work with the vSphere 6.0 Infrastructure

You can use the vSphere 6.0 infrastructure node to configure authentication, licensing, and vCenter Server plug-in settings for vRealize Orchestrator.

Procedure

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

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

3 In the **Component Manager URL** text box, enter the IP address or host name for your infrastructure node.

https://*your_infrastructure_node*/cm

4 In the **Component Manager user name** and **Component Manager password** text boxes, enter the credentials of a vCenter Single Sign-On user with sufficient permissions to query services and register solution users in vCenter Single Sign-On and click **Look up data**.

5 Select the vRealize Orchestrator options you want to configure.

You can later make changes by running workflows in the Orchestrator client, or through the Orchestrator configuration interface.

Option	Action
Import Certificates	Import the vCenter Server certificates. **Import Certificates** must be selected if you are configuring Orchestrator for the first time.
Configure SSO	Change the server mode to **SSO Authentication** and configure a connection to a VMware vCenter Single Sign-On. a Select an Orchestrator administrative domain. b (Optional) Use a filter for the Single Sign-On groups of the selected domain. c Select an Orchestrator administrative group.
Configure Licensing	Select this option if you want to use the vSphere licensing service.
Configure vCenter Server plug-in	Select one or more vCenter Server instances for Orchestrator to connect to.

6 Restart the Orchestrator server service, by clicking **Restart service** in the **Startup Options** tab.

You have successfully configured Orchestrator to work with the vSphere 6.0 infrastructure.

Start the Orchestrator Server

To work with Orchestrator, ensure that the Orchestrator server service has started.

Prerequisites

- If you installed Orchestrator standalone, verify that your system has at least 4 GB of RAM. The Orchestrator server might not start if your system does not meet this requirement.
- Verify that all the status indicators 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 If the Orchestrator server has stopped, click **Start service**.

The Orchestrator server status appears as `Service is starting`. The first boot can take 5-10 minutes because the server is installing the Orchestrator plug-ins content in the database tables.

A message states that the service has started successfully.

4 (Optional) To see the Orchestrator server status, update the page by clicking the **Refresh** link.

The Orchestrator server status can be Running, Not available, and Stopped.

What to do next

Log in to the Orchestrator client, and run or schedule workflows on the vCenter Server inventory objects or other objects that Orchestrator accesses through its plug-ins.

Configuring vRealize Orchestrator in the Orchestrator Appliance 6

Although the Orchestrator Appliance is a preconfigured Linux-based virtual machine, you must 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 "Define the Default SMTP Connection," on page 61 and "Configure the SSH Plug-In," on page 61.

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.

NOTE LDAP authentication is deprecated.

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.

Preconfigured Software	Default User Group (if any) and User	Password
PostgreSQL	User: vmware	vmware
OpenLDAP	User group: vcoadmins User: vcoadmin By default the vcoadmin user is set up as an Orchestrator administrator.	vcoadmin
OpenLDAP	User group: vcousers User: vcouser	vcouser

PostgreSQL and OpenLDAP are suitable for small- to medium-scale production environments. To use the Orchestrator appliance in a large-scale production environment, 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 "Configuring the Orchestrator Database Connection," on page 52. For information about setting up an external directory service or vCenter Single Sign-On, see "Selecting the Authentication Type," on page 42.

Additionally, you can configure the Orchestrator server to work with vCenter Single Sign-On built in the vCenter Server Appliance.

This chapter includes the following topics:

Log In to the Orchestrator Configuration Interface of the Orchestrator Appliance

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

Prerequisites

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

Procedure

1 In a Web browser, go to the IP address of your Orchestrator Appliance virtual machine.

http://*orchestrator_appliance_ip*

2 Click **Orchestrator Configuration**.

3 Log in as vmware and provide the initial Orchestrator Configuration password.

Configure the vCenter Server Plug-In

You can configure Orchestrator to connect to your vCenter Server instances by running the vCenter workflows in the Orchestrator client.

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 same vCenter Single Sign-On instance to which both vCenter Server and vSphere Web Client are pointing. You must also ensure that Orchestrator is registered as a vCenter Server extension. You register Orchestrator as a vCenter Server extension when you specify a user (by providing the user name and password), who has the privileges to manage vCenter Server extensions.

What to do next

Import the SSL certificates for each vCenter Server instance that you defined.

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 a file.

You cannot change the license key and server certificate if you set up Orchestrator to use the embedded database. To change the license key and the server certificate when you use embedded database, you must run the configuration workflows by using either the Orchestrator client or the REST API. For more information about running the configuration workflows by using the Orchestrator client, see *Using the VMware vRealize Orchestrator Plug-Ins*. For detailed instructions about running the configuration workflows by using the REST API, see Chapter 7, "Configuring Orchestrator by Using the Configuration Plug-In and the REST API," on page 79.

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 or a file.

Option	Action
Import from URL	Type the URL of the vCenter Server system: **`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\VMware VirtualCenter\SSL\rui.crt` ■ `/etc/vmware/ssl/rui.crt`

5 Click **Import**.

A message confirming that the import is successful appears.

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

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

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

Option	Action
Host	Type the IP address or the DNS name of the vCenter Server system.
Port	Leave the default value, **443**.
Secure channel	(Optional) Select to establish a secure connection to the vCenter Server system.
Path	Use the default value, **/sdk**.
User name	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 level of the vSphere tree structure.
Password	Type the credentials that Orchestrator must use to establish the connection to vCenter Server.

9 Click **Apply changes**.

10 Restart the Orchestrator server.

Configuring Orchestrator by Using the Configuration Plug-In and the REST API

7

In addition to configuring Orchestrator by using the Orchestrator Web Configuration interface, you can modify the Orchestrator server configuration settings by running workflows included in the Orchestrator Configuration plug-in.

The Configuration plug-in is included by default in the Orchestrator package. You can access the Configuration plug-in workflows from either the Orchestrator workflow library or the REST API. These workflows let you change the settings of the Orchestrator server, such as database, certificates, authentication, and so on. In addition, you can use REST API methods to import and export the Orchestrator server configuration and plug-ins.

Configure the Network Settings

You can modify the IP address that the Orchestrator client interface uses to communicate to the server by running the Configure the network settings workflow in the Configuration plug-in. You can also configure the network settings by using the REST API.

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.

The Configuration plug-in contains a workflow for configuring the Orchestrator network settings. To change the network settings of the Orchestrator server, you can run the Configure the network settings workflow by navigating to **Configuration > Network** in the Workflows view of the Orchestrator client. In addition, you can also run the workflow by using the Orchestrator REST API.

For more information about configuring the Orchestrator database connection by using the Orchestrator configuration interface, see "Configure the Network Connection," on page 39.

Procedure

1 Make a `GET` request at the URL of the Workflow service of the Configure the network settings workflow.

```
GET https://{orchestrator_host}:{port}/vco/api/workflows?conditions=name=Configure network settings
```

2 Retrieve the definition of the workflow by making a `GET` request at the URL of the definition.

To retrieve the definition of the Configure the network settings workflow, make the following `GET` request:

```
GET https://{orchestrator_host}:{port}/vco/api/workflows/440c9173-0866-4819-b4c9-f5e15004fd4c
```

3 Make a `POST` request at the URL that holds the execution objects of the workflow.

For the Configure the network settings workflow, make the following `POST` request:

```
POST https://{orchestrator_host}:
{port}/vco/api/workflows/9643be91-35fc-49a9-819b-56e3bffc7705/executions
```

4 Provide values for the input parameters of the workflow in an execution-context element in the request body.

Option	Description
IP	The IP address to which you want to bind the Orchestrator server
HTTPS	The HTTPS server port

Configuring Authentication Settings by Using the REST API

You can modify the Orchestrator authentication settings when you run the workflows in the Configuration plug-in by using the Orchestrator client or the REST API.

The Configuration plug-in contains workflows that enable you to configure the authentication settings of an Orchestrator server. You can access these workflows by navigating to **Configuration > Authentication** in the Workflows view of the Orchestrator client. In addition, you can also run these workflows by using the Orchestrator REST API. For information about configuring the supported authentication types, see "Selecting the Authentication Type," on page 42.

Configure LDAP Authentication by Using the REST API

You can configure the LDAP authentication settings by running a Configuration workflow or by using the REST API.

NOTE LDAP authentication is deprecated.

To set up an LDAP directory service and configure Orchestrator to work with it, you can run a configuration workflow named after the directory service that you want to set up.

For information about configuring LDAP authentication settings by using the Orchestrator configuration interface, see "Configuring LDAP Settings," on page 46.

Procedure

1 Make a `GET` request at the URL of the Workflow service, for the directory service you want to configure.

Option	Description
Configure Active Directory	Configures Active Directory
Configure eDirectory	Configures eDirectory
Configure Embedded LDAP	Configures Embedded LDAP
Configure OpenLDAP	Configures OpenLDAP
Configure Sun One Directory	Configures Sun ONE Directory

For example, to search for the workflow named Configure Active Directory, make the following `GET` request:

```
GET https://{orchestrator_host}:{port}/vco/api/workflows?conditions=name=Configure Active Directory
```

2 Retrieve the definition of the workflow by making a `GET` request at the URL of the definition.

To retrieve the definition of the Configure Active Directory workflow, make the following `GET` request:

```
GET https://{orchestrator_host}:{port}/vco/api/workflows/fde9fale-lbdd-479f-93fi-0426dd2ad06d
```

3 Make a `POST` request at the URL that holds the execution objects of the workflow.

For the Configure Active Directory workflow, make the following `POST` request:

```
POST https://{orchestrator_host}:{port}/workflows/fde9fale-lbdd-479f-93fi-0426dd2ad06d/executions
```

4 Provide values for the input parameters of the workflow in an execution-context element in the request body.

The following parameters are available for all directory services except Embedded LDAP:

Option	Description
port	The port number
primaryHost	The IP address or the DNS name of the host on which your primary LDAP service runs
secondaryHost	The IP address or the DNS name of the host on which your secondary LDAP service runs
elementRoot	The root element of the LDAP service
useSSL	Activates encrypted certification for the connection between Orchestrator and LDAP
userName	The user name of a valid user who has browsing permissions on your LDAP server

Option	Description
password	The password for the user name
userLookupBase	The LDAP container (the top-level domain name or organizational unit) where Orchestrator searches for potential users
groupLookupBase	The LDAP container where Orchestrator searches for groups
vcoAdminGroup	An LDAP group (such as Domain Users) to which you grant administrative privileges for Orchestrator
requestTimeout	The period within which the Orchestrator server sends a query to the service directory, the directory searches, and sends a reply
dereferenceLinks	Allows all links to be followed before the search operation is performed
filterAttributes	Allows filtering of the attributes that the search returns
hostReachableTimeout	The timeout period for the test checking the status of the destination host

Register Orchestrator as a vCenter Single Sign-On Solution by Using the REST API

You can register the Orchestrator server to work with a vCenter Single Sign-On server by running a Configuration workflow or by using the REST API.

For information about configuring the vCenter Single Sign-On authentication service by using the Orchestrator configuration interface, see "Configuring vCenter Single Sign-On Settings," on page 43.

Procedure

1 Make a `GET` request at the URL of the Configure SSO Workflow service.

```
GET https://{orchestrator_host}:{port}/vco/api/workflows?conditions=name=Configure SSO
```

2 Retrieve the definition of the Configure SSO workflow.

```
GET
https://{orchestrator_host}:{port}/vco/api/workflows/9ff67fbc-411c-47c7-af80-c81b1215b516
```

3 Make a `POST` request at the URL that holds the execution objects of the Configure SSO workflow.

```
POST
https://{orchestrator_host}:{port}/vco/api/workflows/9ff67fbc-411c-47c7-af80-
c81b1215b516/executions
```

4 Provide values for the input parameters of the workflow in an execution-context element in the request body.

Option	Description
mode	The authentication mode
ssoHost	The URL of the machine on which vCenter Single Sign-On is installed
ssoPort	The vCenter Single Sign-On server port
tokenServiceURL	The URL for the vCenter Single Sign-On token service interface
adminServiceURL	The URL for the vCenter Single Sign-On administration service interface
ssoAdminUser	The vCenter Single Sign-On administrator user name
ssoAdminPassword	The vCenter Single Sign-On administrator password
clockTolerance	The time difference between a client clock and a domain controller clock
vcoAdminGroup	The Orchestrator administrator domain group

Configure the Database Connection by Using the REST API

You can modify the Orchestrator database connection when you run a workflow from the Configuration plug-in. You can also configure the database connection by using the REST API.

The Configuration plug-in contains workflows for configuring the database types supported by Orchestrator. To change the settings of the Orchestrator database connection, you can run a workflow named after the database type you want to configure. You can find these workflows by navigating to **Configuration > Database** in the Workflows view of the Orchestrator client. In addition, you can also run these workflows by using the Orchestrator REST API.

For more information about configuring the Orchestrator database connection by using the Orchestrator configuration interface, see "Configure the Database Connection," on page 54.

Procedure

1 Make a `GET` request at the URL of the Workflow service, for the database connection you want to configure.

Option	Description
Oracle	Configures Orchestrator to work with an Oracle database instance
Microsoft SQL Server	Configures Orchestrator to work with a Microsoft SQL Server or Microsoft SQL Server Express database instance
PostgreSQL	Configures Orchestrator to work with a PostgreSQL database instance
Embedded	Configures Orchestrator to work with the embedded database

For example, to search for a workflow named Microsoft SQL Server, make the following `GET` request:

```
GET https://{orchestrator_host}:{port}/vco/api/workflows?conditions=name=Microsoft SQL Server
```

2 Retrieve the definition of the workflow by making a `GET` request at the URL of the definition.

To retrieve the definition of the Microsoft SQL Server workflow, make the following `GET` request:

```
GET https://{orchestrator_host}:{port}/vco/api/workflows/9643be91–35fc–49a9–819b–56e3bffc7705
```

3 Make a `POST` request at the URL that holds the execution objects of the workflow.

For the Microsoft SQL Server workflow, make the following `POST` request:

```
POST https://{orchestrator_host}:
{port}/vco/api/workflows/9643be91–35fc–49a9–819b–56e3bffc7705/executions
```

4 Provide values for the input parameters of the workflow in an execution-context element in the request body.

Option	Description
`host`	The database server IP address or DNS name. This parameter is applicable for all databases.
`port`	The database server port that allows communication to your database. This parameter is applicable for all databases.
`databaseName`	The full unique name of your database. The database name is specified by the `SERVICE_NAMES` parameter in the initialization parameter file. This parameter is valid only for SQL Server, and PostgreSQL workflows.
`db`	The name of the database instance that can be identified by the `INSTANCE_NAME` parameter in the database initialization parameter file. This parameter is valid only for SQL Server and Oracle databases.

Option	Description
domain	To use Windows authentication, type the domain name of the SQL Server machine, for example **company.org**. To use SQL authentication, provide an empty value for this parameter. This parameter is valid only for SQL server and specifies whether you want to use Windows or SQL Server authentication.
ntlm2	Select to send NTLMv2 responses when using Windows authentication. This parameter is valid only for SQL Server.
user	The user name that Orchestrator uses to connect and operate the selected database. The name you type must be a valid user on the target database with **db_owner** rights. This parameter is applicable for all databases.
password	The password for the user name. This parameter is applicable for all databases.
ssl	Specifies whether you want to use SSL connection to the database. To use this parameter, you must import the database SSL certificate into Orchestrator. This parameter is applicable for all databases.

Create a Self-Signed Server Certificate by Using the REST API

You can create a self-signed certificate by running a workflow from the Configuration plug-in or by using the REST API.

The Configuration plug-in contains a workflow for creating a certificate database and inserting a self-signed server certificate in it. You can access this workflow by navigating to **Configuration > Package Signing Certificate** folder in the Workflows view of the Orchestrator client. In addition, you can also run this workflow by using the Orchestrator REST API.

For information about creating a certificate database and a self-signed server certificate by using the Orchestrator configuration interface, see "Create a Self-Signed Server Certificate," on page 57.

Procedure

1 Make a `GET` request at the URL of the Workflow service of the Create a certificate database and a self-signed server certificate workflow.

```
GET https://{orchestrator_host}:{port}/vco/api/workflows?conditions=name=Create a
certificate database and a self-signed server certificate
```

2 Retrieve the definition of the Create a certificate database and a self-signed server certificate workflow by making a `GET` request at the URL of the definition.

```
GET https://{orchestrator_host}:{port}/vco/api/workflows/4d6b34ee-86f7-4a30-8ca0-c8d56ac0f74b
```

3 Make a `POST` request at the URL that holds the execution objects of the Create a certificate database and a self-signed server certificate workflow.

```
POST https://{orchestrator_host}:{port}/vco/api/workflows/4d6b34ee-86f7-4a30-8ca0-
c8d56ac0f74b/executions
```

4 Provide values for the input parameters of the Create a certificate database and a self-signed server certificate workflow in an execution-context element in the request body.

Option	Description
commonName	The common name of the certificate that consists of at least six characters
organization	The name of the organization

Option	Description
`organizationalUnit`	The name of the organization unit
`country`	The country code (two characters)

Managing SSL Certificates by Using the REST API

In addition to managing SSL certificates by using the Orchestrator configuration interface, you can also manage trusted certificates when you run workflows from the Configuration plug-in or by using the REST API.

The Configuration plug-in contains workflows for importing and deleting SSL certificates. You can access these workflows by navigating to **Configuration > SSL Trust Manager** in the Workflows view of the Orchestrator client. In addition, you can also run these workflows by using the Orchestrator REST API.

Delete an SSL Certificate by Using the REST API

You can delete an SSL certificate by running the Delete trusted certificate workflow of the Configuration plug-in or by using the REST API.

Procedure

1 Make a `GET` request at the URL of the Workflow service of the Delete trusted certificate workflow.

```
GET https://{orchestrator_host}:{port}/vco/api/workflows?conditions=name=Delete trusted certificate
```

2 Retrieve the definition of the Delete trusted certificate workflow by making a `GET` request at the URL of the definition.

```
GET https://{orchestrator_host}:{port}/vco/api/workflows/8a70a326-ffd7-4fef-97e0-2002ac49f5bd
```

3 Make a `POST` request at the URL that holds the execution objects of the Delete trusted certificate workflow.

```
POST https://{orchestrator_host}:{port}/vco/api/workflows/8a70a326-ffd7-4fef-97e0-2002ac49f5bd/executions/
```

4 Provide the name of the certificate you want to delete as an input parameter of the Delete trusted certificate workflow in an execution-context element in the request body.

Import SSL Certificates by Using the REST API

You can import SSL certificates by running a workflow from the Configuration plug-in or by using the REST API.

You can import a trusted certificate from a file or a URL. For information about importing the vCenter Server SSL certificate by using the Orchestrator configuration interface, see "Import the vCenter Server SSL Certificate," on page 41.

Procedure

1 Make a `GET` request at the URL of the Workflow service.

Option	Description
Import trusted certificate from a file	Imports a trusted certificate from a file.
Import trusted certificate from URL	Imports a trusted certificate from a URL address.

Option	Description
Import trusted certificate from URL using proxy server	Imports a trusted certificate from a URL address by using a proxy server.
Import trusted certificate from URL with certificate alias	Imports a trusted certificate with a certificate alias, from a URL address.

To import a trusted certificate from a file, make the following `GET` request:

```
GET https://{orchestrator_host}:{port}/vco/api/workflows?conditions=name=Import
                trusted certificate from a file
```

2 Retrieve the definition of the workflow by making a `GET` request at the URL of the definition.

To retrieve the definition of the Import trusted certificate from a file workflow, make the following `GET` request:

```
GET https://{orchestrator_host}:{port}/vco/api/workflows/93a7bb21-0255-4750-9293-2437abe9d2e5
```

3 Make a `POST` request at the URL that holds the execution objects of the workflow.

For the Import trusted certificate from a file workflow, make the following `POST` request:

```
POST https://{orchestrator_host}:
{port}/vco/api/workflows/93a7bb21-0255-4750-9293-2437abe9d2e5/executions
```

4 Provide values for the input parameters of the workflow in an execution-context element of the request body.

Parameter	Description
cer	The CER file from which you want to import the SSL certificate. This parameter is applicable for the Import trusted certificate from a file workflow.
url	The URL from which you want to import the SSL certificate. For non-HTPS services, the supported format is *IP_address_or_DNS_name:port*. This parameter is applicable for the Import trusted certificate from URL workflow.

Importing Licenses by Using the REST API

You can import licenses by running a Configuration plug-in workflow or by using the REST API.

The Configuration plug-in contains workflows that let you import the vCenter Server license and enter license keys. You can access these workflows by navigating to **Configuration > VMware > License** in the Workflows view of the Orchestrator client. In addition, you can also run these workflows by using the Orchestrator REST API.

Import the vCenter Server License by Using the REST API

You can import the vCenter Server license by running a workflow from the Configuration plug-in or by using the REST API.

Procedure

1 Make a `GET` request at the URL of the Workflow service of the Use vCenter Server license workflow.

```
GET https://{orchestrator_host}:{port}/vco/api/workflows?conditions=name=Use vCenter server
license
```

2 Retrieve the definition of the Use vCenter Server license workflow by making a `GET` request at the URL of the definition.

```
GET https://{orchestrator_host}:{port}/vco/api/workflows/5f4a37f4-6f8f-4d20-9468-e7018c206952
```

3 Make a `POST` request at the URL that holds the execution objects of the Use vCenter Server license workflow.

```
POST https://{orchestrator_host}:{port}/vco/api/workflows/5f4a37f4-6f8f-4d20-9468-
e7018c206952/executions/
```

4 Provide values for the input parameters of the Use vCenter Server license workflow in an execution-context element in the request body.

Option	Description
host	The IP address or DNS name of the vCenter Server host.
port	The port number of the vCenter Server host.
user name	The user name that Orchestrator must use to establish connection to vCenter Server. The user must have administrative privileges on your vCenter Server instance.
password	The password for authenticating on the vCenter Server instance.

Enter a License Key by Using the REST API

You can import a license key by running a workflow from the Configuration plug-in or by using the REST API.

Procedure

1 Make a `GET` request at the URL of the Workflow service of the Enter license key workflow.

```
GET https://{orchestrator_host}:{port}/vco/api/workflows?conditions=name=Enter license key
```

2 Retrieve the definition of the Enter license key workflow by making a `GET` request at the URL of the definition.

```
GET https://{orchestrator_host}:{port}/vco/api/workflows/780cb259-a137-46ca-a232-7e06c413af8c
```

3 Make a `POST` request at the URL that holds the execution objects of the Enter license key workflow.

```
POST https://{orchestrator_host}:{port}/vco/api/workflows/780cb259-a137-46ca-
a232-7e06c413af8c/executions/
```

4 Provide values for the input parameters of the Enter license key workflow in an execution-context element in the request body.

Option	Description
owner	The license owner
serial	The license serial number

8 Additional Configuration Options

You can use the Orchestrator configuration interface to change the default Orchestrator behavior.

This chapter includes the following topics:

Change the Password of the Orchestrator Configuration Interface

You can change the Orchestrator configuration interface password at anytime to avoid potential security issues.

Prerequisites

Verify that the VMware vRealize Orchestrator Configuration service is running.

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 your current password.

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

5 Reenter the new password to confirm it.

6 Click **Apply changes**.

Uninstall a Plug-In

You can use the Orchestrator configuration interface to disable a plug-in, but this does not remove the plug-in file from the 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.

Procedure

1 Log in as an administrator to the machine on which the Orchestrator server is installed.

2 Navigate to the Orchestrator plug-in installation folder.

Option	Action
If you installed Orchestrator standalone	Go to *install_directory*\VMware\Orchestrator\app-server\conf\plugins
If you installed Orchestrator Appliance	Go to *install_directory*/etc/vco/app-server/plugins

3 Delete the `.dar` and `.war` archives that contain the plug-in you want to remove.

4 Restart the vRealize Orchestrator services.

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

5 Delete the plug-in configuration files.

Option	Action
If the plug-in configuration is stored in a configuration file in the default configuration directory	Delete the plug-in configuration file. ■ If you installed Orchestrator standalone, delete that file from *install_directory*\VMware\Orchestrator\app-server\conf\plugins ■ If you installed Orchestrator Appliance, delete that file from *install_directory*/etc/vco/app-server/plugins
If the plug-in has a configuration tab in the Orchestrator configuration interface	Remove the configuration tab by deleting the related files. ■ If you installed Orchestrator standalone, delete the files from *install_directory*\configuration\webapps ■ If you installed Orchestrator Appliance, delete the files from *install_directory*/usr/lib/vco/configuration/webapps

6 Log in to the Orchestrator client.

7 Select **Administer** from the drop-down menu in the left upper corner.

8 Click the **Packages** view.

9 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.

10 Click **Delete all**.

11 Restart the vRealize Orchestrator services.

You removed all custom workflows, actions, policies, configurations, settings, and resources related to the plug-in.

Export the Orchestrator Configuration

The Orchestrator configuration interface provides a mechanism to export the Orchestrator configuration 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.

You should export and save your configuration settings on a regular basis, especially when making modifications, performing maintenance tasks, or upgrading the system.

For a list of exported configuration settings, see "Orchestrator Configuration Files," on page 91.

IMPORTANT Keep the file with the exported configuration safe and secure, because it contains sensitive administrative information.

Procedure

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

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

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

Use the same password when you import the configuration.

4 Click **Export**.

Orchestrator creates a `vmo_config_dateReference.vmoconfig` file on the machine on which the Orchestrator server is installed. You can use this file to clone or to restore the system.

Orchestrator Configuration Files

When you export the system configuration, a `vmo_config_dateReference.vmoconfig` file is created locally on the machine on which the Orchestrator server is installed. 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 unique for each machine where the Orchestrator server is installed. These empty files must be reconfigured, even when a working configuration was previously imported.

Table 8-1. Settings Not Saved During Configuration Export

Setting	Description
Licenses	Manually imported licenses are not exported. They are stored in the Orchestrator database.
Server	The server configuration is reset to Unknown. You must install the Orchestrator server as a Windows service again.

Table 8-2. Settings Saved During Configuration Export

Setting	Description
passwordencryptor.key	The key used to encrypt the sensitive data. If the file is not valid, the sensitive data hashes stored in the database become unusable.
General	The expiration time period of completed events and the maximum number of workflows recorded.
Network	The IP binding address and the TCP ports used by the different elements of the Orchestrator server.
Database	The database configuration.

Table 8-2. Settings Saved During Configuration Export (Continued)

Setting	Description
Certificate	The certificates added as trusted authorities.
Authentication	The Signle Sign-On or LDAP server configuration.
Log	The log settings information.
Plug-ins	The list of disabled plug-ins and the account name.
Mail plug-in	The SMTP host, SMTP port, user name, password, sender's name, and sender's email address.
vCenter Server plug-in	The vCenter Server plug-in configuration. Each vCenter Server plug-in has an ID element , for example <guid>36907986-d951-4f9a-9542-c561f4b94c3f</guid>, which is used as an identifier of the vCenter Server instance. In case you do not use the export for backup purposes, make sure that you change the unique ID of the vCenter Server plug-in.
License	The details about the vCenter Server host on which Orchestrator verifies the license key.
jssecacerts	The certificates added as trusted authorities.
dunes-pk	The internal private key generated for each Orchestrator server instance. It is used as an identifier. The vCenter Server plug-in uses this key to register to the vCenter Server instances and uses it for logging in to the vCenter Server instances. If the key changes, the vCenter Server plug-in cannot log in anymore.

Import the Orchestrator Configuration

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

If you use the import procedure for cloning the Orchestrator configuration, the vCenter Server plug-in configuration becomes invalid and non-working, because a new ID of the vCenter Server plug-in is generated. After you import the Orchestrator configuration, you must provide a valid password for each registered vCenter Server instance.

Procedure

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

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

3 Type the password you used when exporting the configuration.

This step is not necessary if you have not specified a password.

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

5 Select whether to override the Orchestrator internal certificate and network settings.

Select the check box only if you want to restore your Orchestrator configuration and the `.vmoconfig` file is the backup file of the same Orchestrator configuration.

If you import the configuration to duplicate the Orchestrator environment, for example for scaling purposes, leave the check box unselected. Otherwise you might have problems with the certificates when Orchestrator tries to identify against vCenter Server, vCenter Single Sign-On or the vSphere Web Client.

6 Click **Import**.

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

Configure the Expiration Period of Events and the Maximum Number of Runs

You can define the expiration period of events stored in the Orchestrator 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 for a specified time period. When the specified time period expires for an event, the database deletes the 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 In the **Expiration days of log events** text box, type an integer value for the number of days, for which you want to store events.

4 Fill in the **Maximum 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, type **0** in this text box. If you type **0**, your database continues to extend.

5 Click **Apply changes**.

Import Licenses for a Plug-In

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.

To import license keys when you use the embedded database, you must run the Enter license key configuration workflow by using either the Orchestrator client or the REST API. For more information about running the configuration workflows by using the Orchestrator client, see *Using the VMware vRealize OrchestratorPlug-Ins*. For detailed instructions about running the configuration workflows by using the REST API, see Chapter 7, "Configuring Orchestrator by Using the Configuration Plug-In and the REST API," on page 79.

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 In the **License owner** text box, type the name of the license owner.

6 Click **Apply changes**.

What to do next

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

Orchestrator Log Files

VMware Technical Support routinely requests diagnostic information from you when you submit a support request. This diagnostic information contains product-specific logs and configuration files from the host on which the product runs. The information is gathered by using a specific script tool for each product.

Table 8-3. Orchestrator Log Files list

File Name	Location	Description
`scripting.log`	■ If you installed Orchestrator standalone: *`install_directory`*`\VMware\Orchestrator\app-server\logs` ■ If you deployed the Orchestrator Appliance: `/var/log/vco/app-server`	Provides a list of the completed workflows and actions. The `scripts-logs.log` file lets you isolate workflow runs and actions runs from normal Orchestrator operations. This information is also included in the `server.log` file.
`server.log`	■ If you installed Orchestrator standalone: *`install_directory`*`\VMware\Orchestrator\app-server\logs` ■ If you deployed the Orchestrator Appliance: `/var/log/vco/app-server`	Provides information about all activities on the Orchestrator server. Analyze the `server.log` file when you debug Orchestrator or any application that runs on Orchestrator.
`wrapper-configuration.log`	On the Orchestrator standalone: *`install_directory`*`\VMware\Orchestrator\configuration\logs`	Provides information about the configuration and validation of each component of Orchestrator.
`catalina.out`	On the Orchestrator Appliance: `/var/log/vco/configuration/`	Provides information about the configuration and validation of each component of Orchestrator in the Orchestrator Appliance. The file is analogous to `wrapper-configuration.log` in the Windows installation of Orchestrator.
`vso.log`	■ If you installed Orchestrator standalone: *`install_directory`*`\VMware\Orchestrator\apps` ■ If you installed the Orchestrator client on a Mac machine: *`install_directory`* ■ If you installed the Orchestrator client on a Linux machine: *`install_directory`*	This is the Orchestrator client log. Use this log to detect connection problems with the server and detect events on the client side. It is not available for the Orchestrator Appliance.
`access.yyyy-mm-dd.log`	■ If you installed Orchestrator standalone: *`install_directory`*`\VMware\Orchestrator\configuration\logs` ■ If you deployed the Orchestrator Appliance: `/var/log/vco/app-server`	This log lists the elements that are needed to load and display the pages of the Orchestrator configuration interface. It contains a history of the tasks you performed while configuring Orchestrator along with the time they were completed. However, the log does not display the value of the changed parameters. Use this log to identify changes in the behavior of the Orchestrator server after a restart.

Table 8-3. Orchestrator Log Files list (Continued)

File Name	Location	Description
`wrapper.log`	If you installed Orchestrator standalone: *`install_directory`*`\VMware\Orchestrator\app-server\bin`	Provides a part of the boot log information of the server. Use this log to check whether the VMware vRealize Orchestrator Server service was started by the wrapper or by a user.
`metrics.log`	■ If you installed Orchestrator standalone: *`install_directory`*`\VMware\Orchestrator\app-server\logs` ■ If you deployed the Orchestrator Appliance: `/var/log/vco/app-server`	Contains runtime information about the server. The information is added to this log file once every 5 minutes.
`localhost_access_log.txt`	■ If you installed Orchestrator standalone: *`install_directory`*`\VMware\Orchestrator\app-server\logs` ■ If you deployed the Orchestrator Appliance: `/storage/log/vmware/vco/app-server`	This is the HTTP request log of the server.

Logging Persistence

You can log information in any Orchestrator script (workflow, policy, or action). This information has types and levels. The type can be either persistent or non-persistent. The level can be `DEBUG`, `INFO`, `WARNING`, and `ERROR`.

Table 8-4. Creating Persistent and Non-Persistent Logs

Log Level	Persistent Type	Non-Persistent Type
`DEBUG`	Server.debug("short text", "long text");	N/A
`INFO`	Server.log("short text", "long text");	System.log("text");
`WARNING`	Server.warn("short text", "long text");	System.warn("text");
`ERROR`	Server.error("short text", "long text");	System.error("text");

Persistent Logs

Persistent logs (server logs) track past workflow run logs and are stored in the Orchestrator database. To view server logs, you must select a workflow, a completed workflow run, or policy and click the **Events** tab in the Orchestrator client.

Non-Persistent Logs

When you use a non-persistent log (system log) in your scripting, the Orchestrator server notifies all running Orchestrator applications about this log, but this information is not stored. When the application is restarted, the log information is lost. Non-persistent logs are used for debugging purposes or for live information. To view system logs, you must select a completed workflow run in the Orchestrator client and click **Logs** on the **Schema** tab.

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 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.

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

NOTE The log 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\log\.

Change the Size of Server Logs

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

Procedure

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

Option	Action
If you installed the standalone version of Orchestrator	Go to *install_directory*\VMware\Orchestrator\app-server\conf.
If you downloaded and deployed the virtual appliance	Go to /etc/vco/app-server/.

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

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

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

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

3 Change the following lines:

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

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

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

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

Export Orchestrator Log Files

Orchestrator provides a workflow that generates a ZIP archive of troubleshooting information containing configuration, server, wrapper, and installation log files.

Prerequisites

Verify that you created the `c:/orchestrator` folder at the root of the Orchestrator server system or set write access rights to another folder in which to store the generated ZIP archive. See "Set Server File System Access for Workflows and JavaScript," on page 115.

You must be logged in to the Orchestrator client as a member of the Orchestrator administrator group.

Procedure

1 Click the **Workflows** view in the Orchestrator client.

2 In the workflows hierarchical list, open **Library > Troubleshooting** and navigate to the Export logs and application settings workflow.

3 Right-click the Export logs and application settings workflow and select **Start workflow**.

4 (Optional) Type the path to the folder on the Orchestrator server in which to store the output ZIP archive.

If you do not type a path, the generated ZIP archive is stored in the `c:/orchestrator` folder.

5 Click **Submit** to run the workflow.

The troubleshooting information is stored in a ZIP archive named `vCO_troubleshooting_`*`dateReference_xxxxxx`*`.zip`.

Filter the Orchestrator Log Files

You can filter the Orchestrator server logs for a specific workflow run and collect diagnostic data about the workflow run.

The Orchestrator logs contain a lot of useful information, but not every log entry has diagnostic context. When multiple instances of the same workflow are running at the same time, you can track the different workflow runs by filtering the diagnostic data about each run in the Orchestrator logs.

Procedure

1 Log in as an administrator to the machine on which the Orchestrator server is installed.

2 Navigate to the *install_directory*\VMware\Infrastructure\Orchestrator\app-server\conf\log4j.xml file and open it in a text editor.

3 Find the following entry:

```
<layout class="org.apache.log4j.PatternLayout"> <param
name="ConversionPattern" value="%d{yyyy-MM-dd HH:mm:ss.SSSZ} %-5p
[%c{1}] %m%n"/> </layout>
```

4 Change the conversion pattern.

```
<layout class="org.apache.log4j.PatternLayout"> <param
name="ConversionPattern" value="%d{yyyy-MM-dd HH:mm:ss.SSSZ} %-5p
[%c{1}][%X{value_name}] %m%n"/> </layout>
```

Where *value_name* is the name of the available diagnostic values. The possible names are:

Option	Description
username	The name of the user who started the workflow
workflowName	The name of the running workflow
workflowId	The ID of the running workflow
token	The token of the running workflow
process	The workflow ID and token, separated by a colon
full	The name of the user who started the workflow, the name of the running workflow, the workflow ID, and the workflow token, separated by colons.

5 Save and close the file.

The Orchestrator logs are filtered according to the changes you made to the file.

Configuration Use Cases and Troubleshooting

9

You can configure the Orchestrator server to work with the vCenter Server appliance, you can also uninstall plug-ins from Orchestrator, or change the self-signed certificates.

The configuration use cases provide task flows that you can perform to meet specific configuration requirements of your Orchestrator server, as well as troubleshooting topics to understand and solve a problem, if a workaround exists.

This chapter includes the following topics:

Registering Orchestrator with vCenter Single Sign-On in the vCenter Server Appliance

If you want to configure Orchestrator to work with the VMware vCenter Server Appliance, and want to run workflows by using the vSphere Web Client, you must configure the Orchestrator server to work with vCenter Single Sign-On, which is prebuilt in the appliance.

IMPORTANT Ensure that the clocks of the Orchestrator server machine and the vCenter Server Appliance are synchronized. Otherwise you might receive cryptic vCenter Single Sign-On errors.

This workflow describes the process to change the self-signed certificate.

1 Download and deploy the VMware vCenter Server Appliance.

  See *vSphere Installation and Setup* for instructions.

2 Import the SSL and vCenter Single Sign-On certificates of the vCenter Server instance running in the vCenter Server Appliance into Orchestrator.

You import certificates from the Orchestrator configuration interface. For more information about importing certificates, see "Import the vCenter Server SSL Certificate," on page 41 and "Import the vCenter Single Sign-On SSL Certificate," on page 43.

- For importing the SSL certificate of the vCenter Server instance running in the appliance, in the **Import from URL** text box, type ***your_vcenter_server_appliance_ip_address:vcenter_server_api_port***.
- For importing the vCenter Single Sign-On certificate, in the **Import from URL** text box, type ***your_vcenter_server_appliance_ip_address:single_sign_on_port***.

3 In the Orchestrator configuration interface, click **Authentication** and select **SSO Authentication**.

4 Register Orchestrator to work with vCenter Single Sign-On:

a In the **Host** text box, type ***your_vcenter_server_appliance_ip_address*:443**

b In the **Admin user name** and the **Admin password** text boxes, type the credentials of the root user of the vCenter Server Appliance.

c Click **Register Orchestrator**.

d Complete the registration by selecting the Orchestrator administrator domain and group from the drop-down menu.

Setting Up Orchestrator to Work with the vSphere Web Client

You must configure Orchestrator so that you can use the vSphere Web Client to log in to Orchestrator and run workflows on the objects in your vSphere inventory.

1 Install vCenter Single Sign-On, vCenter Server, and vRealize Orchestrator.

Orchestrator is silently installed on your system when you install vCenter Server. For more information about installing vCenter Single Sign-On and vCenter Server, see *vSphere Installation and Setup*.

2 Configure the vSphere Web Client to work with vCenter Single Sign-On, which you have installed in the previous step.

For more information, see *vSphere Installation and Setup*.

3 Start the Orchestrator Configuration Service and log in to the Orchestrator configuration interface.

You installed Orchestrator as a part of the vCenter Server installation, and the Orchestrator Configuration service does not start by default. You must start it manually before you attempt to access the Orchestrator configuration interface. For instructions, see "Start the Orchestrator Configuration Service," on page 38 and "Log In to the Orchestrator Configuration Interface," on page 39.

4 Select the correct IP address from the **IP address** drop-down menu on the **Network** tab in the Orchestrator configuration interface.

5 Verify that the vCenter Server plug-in in the Orchestrator configuration interface is properly configured, provide the credentials of a user who has the privileges to manage vCenter Server extensions, and save the changes.

You must add your vCenter Server instance as a host. For more information, see "Configure the vCenter Server Plug-In," on page 62.

6 Start the Orchestrator server.

For more information, see "Start the Orchestrator Server," on page 72.

7 If there is more than one Orchestrator managing this vCenter Server instance, log in to the vSphere Web Client and configure the default vCenter Orchestrator instance.

IMPORTANT You must log in as a user who has at least **View** and **Execute** permissions in Orchestrator, and permissions to manage vCenter Server objects.

If you want to see more workflows displayed in the pop-up menu when you right-click a vSphere inventory object, you can associate workflows with the different vSphere object types.

For more information, see *vCenter Server and Host Management*.

You can now use the vSphere Web Client to run Orchestrator workflows on the objects in your vSphere inventory.

Check Whether Orchestrator Is Successfully Registered as an Extension

After you register Orchestrator server with vCenter Single Sign-On and configure it to work with vCenter Server, you can check whether Orchestrator is successfully registered as an extension with vCenter Server.

Procedure

1 In a Web browser navigate to the managed object browser of your vCenter Server instance.

https://*your_vcenter_server_ip*/mob

2 Log in with your vCenter Server credentials.

3 Under Properties, click **content**.

4 On the Data Object Type: ServiceContent page, under Properties, click **ExtensionManager**.

5 On the Managed Object Type page, under Properties, click the Orchestrator extension string.

extensionList["com.vmware.vco"]

The extension has a `server` property which contains an array of type `ExtensionServerInfo`. The array should contain an instance of the `ExtensionServerInfo` type with a `url` property which contains the URL of the registered Orchestrator server.

6 On the Data Object Type: Extension page, under Properties, click **server**.

You can see information about the Orchestrator server registered as an extension, such as `serverThumbprint` and `url`. The `serverThumbprint` property is the SHA-1 thumbprint of the Orchestrator server certificate, which is a unique identifier of the Orchestrator server. The `url` property is the service URL of the Orchestrator server. There is one record per IP address. If the Orchestrator server has two IP addresses, both of them are displayed as service URLs.

Unregister Orchestrator from vCenter Single Sign-On

You can unregister Orchestrator from vCenter Single Sign-On, for example, when you no longer want to use the vSphere Web Client, when you want to change vCenter Single Sign-On with LDAP, or when you want to register Orchestrator with another vCenter Single Sign-On instance.

NOTE LDAP authentication is deprecated.

Procedure

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

2 Click **Authentication**.

3 Type the administrator password in the **Admin password** text box.

The **Host** and **Admin name** text boxes must contain the values you typed when you registered Orchestrator with vCenter Single Sign-On.

4 Click **Unregister Orchestrator**.

If for some reason the operation cannot be completed, for example if the vCenter Single Sign-On server is not running, delete the vCenter Single Sign-On configuration data stored locally on your system by clicking **Delete SSO configuration**.

What to do next

You can register Orchestrator with another vCenter Single Sign-On server or change the authentication type to LDAP authentication.

Create an Archive for Upgrading Orchestrator

If you upgrade Orchestrator by upgrading vCenter Server 5.0 or later to vCenter Server 6.0, the `vco_export.zip` archive, located at `%VMWARE_CIS_HOME%/vco` might not get created automatically and your configuration might not be migrated.

Problem

During the export phase of the upgrade, Orchestrator upgrade script collects configuration files and data, and stores them in the `vco_export.zip` archive. In some cases the archive might not be created automatically and must be created manually if you want to preserve the data after the update.

Cause

During an export, Orchestrator accesses the Windows registry to find the necessary data. If Orchestrator cannot access that data, the automatic export does not occur.

Solution

1 Create the `vco_export.zip` archive manually with the necessary data, and save it to `%VMWARE_CIS_HOME%/vco`.

The export archive must contain the following files:

File	Location	Description
Plug-in DAR files	■ On Orchestrator 5.5.x: *install_directory*\VMware\Orchestrator\app-server\plugins ■ On Orchestrator 5.1 or earlier: *install_directory*\VMware\Orchestrator\app-server\server\vmo\plugins	A copy of the plug-in `.dar` files. During the import phase, plug-ins are not downgraded. Orchestrator imports only the plug-in configuration but a `.dar` file is not substituded by an earlier version. If a source plug-in is not installed on the destination system, it is imported and disabled. Source plug-ins might not be verified for Orchestrator 6.0.1 and might cause errors.
`vmo_config.zip`	The location varies. After you export the file, you receive a message with the location of the file.	This file has the same content as the `.vmoconfig` file generated by the Orchestrator Configuration's **Export Configuration** option found on the **General** tab.

File	Location	Description
Properties files	■ On Orchestrator 5.5.x: *install_directory*\VMware\Orchestrator\app-server\conf ■ On Orchestrator 5.1 or earlier: *install_directory*\VMware\Orchestrator\app-server\server\vmo\conf	All of the `.properties` files located in the folder. The folder may also include custom defined properties. The file `sso.properties` is present only if the source system is configured to use Single Sign-On.
`jssecacerts`	On Orchestrator 4.2.x: *install_directory*\VMware\Orchestrator\jre\lib\security\jssecacerts	This file is included only in Orchestrator 4.2.x. In later versions, the file is a part of `vmo_config.zip`. It contains the Certificate Authorities certificates, which are imported through the Orchestrator configuration interface.

2 Use the archive to migrate your configuration.

a Log in to the Orchestrator configuration interface as **`vmware`**.

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

c Type the password you used when exporting the configuration.

This step is not necessary if you have not specified a password.

d Browse to select the `vco_export.zip` file.

e Select whether to override the Orchestrator internal certificate and network settings.

Select the check box only if you want to restore your Orchestrator configuration and the `vco_export.zip` file is the backup file of the same Orchestrator configuration.

If you import the configuration to duplicate the Orchestrator environment, for example for scaling purposes, leave the check box unselected. Otherwise you might have problems with the certificates when Orchestrator tries to identify against vCenter Server, vCenter Single Sign-On or the vSphere Web Client.

f Click **Import**.

Changing SSL Certificates

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

When you attempt to use Orchestrator over a trusted SSL Internet connection, and you open the Orchestrator configuration interface in a Web browser, you receive warnings that the connection is untrusted (in Mozilla Firefox) or that problems have been detected with the Web site's security certificate (in Internet Explorer).

After you click **Continue to this website (not recommended)**, even if you have imported the SSL certificate as a trusted store, you continue to see the Certificate Error red notification in the address bar of the Web browser. You can work with Orchestrator in the Web browser, but a third-party system might not work properly when attempting to access the API over HTTPS.

You can also receive a certificate warning when you start the Orchestrator client and attempt to connect to the Orchestrator server over an SSL connection.

You can resolve the problem by installing a certificate signed by a commercial certificate authority (CA) or by creating a certificate that matches your Orchestrator server name and then importing the certificate in your local keystore. To stop receiving a certificate warning from the Orchestrator client, add your root CA certificate to the Orchestrator keystore on the machine on which the Orchestrator client is installed.

Generate a New Certificate

If you plan to change an SSL certificate, you can generate a new certificate. You can generate the new certificate on the same computer on which Orchestrator is installed or on another computer.

Prerequisites

- Run the Java `keytool` utility. You can find the utility on the system on which Orchestrator is installed.
- Back up the `jssecacerts` file, located at *`install_directory`*`\app-server\conf\security\jssecacerts`.

Procedure

1. Stop the Orchestrator server service.
   a. Select **Start > Programs > Administrative Tools > Services**.
   b. In the right pane, right-click **VMware vRealize Orchestrator Server** and select **Stop**.
2. On the Windows **Start** menu, right-click **Command Prompt**, and select **Run as administrator**.
3. Navigate to the `keytool` utility located at *`install_directory`*`\VMware\CIS\jre\bin\keytool`.
4. Delete the current dunes key from the keystore.

   ```
   keytool -delete -alias dunes -keystore "install_directory\app-
   server\conf\security\jssecacerts"
   ```

5. Generate a new certificate for the dunes key, for example a 10-years certificate:

   ```
   keytool -keystore "install_directory\app-server\conf\security\jssecacerts" -storepass
   dunesdunes -genkey -keyalg RSA -alias dunes -validity 3650
   ```

   You can adjust the validity of the certificate in days.

6 When prompted for your first and last name, enter the fully qualified domain name (FQDN) of your Orchestrator server.

Make sure to enter the FQDN of the Orchestrator server. For example, if the FQDN of the Orchestrator server is **orchestrator.lab**, you need to type the following information:

```
What is your first and last name?

    [Unknown]: orchestrator.lab
```

7 For each of the remaining prompts such as Organizational Unit, Organization, City, State, Country Code, and so on, type the appropriate information for your organization.

8 To confirm the change, type **yes**, and press Enter.

9 When prompted for the password for dunes, press Enter to use the same password as the keystore password (dunesdunes).

10 Log in to the Orchestrator configuration interface as vmware and start the Orchestrator server service.

a In the Orchestrator configuration interface, click the **Startup Options** tab.

b Click **Start service**.

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

Prerequisites

Generate a new SSL certificate.

Procedure

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

```
keytool –certreq –alias dunes –keypass "dunesdunes" –keystore
        "install_directory\app-server\conf\security\jssecacerts" –storepass
        "dunesdunes" –file certreq.csr
```

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 Import the SSL certificate into 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 the following command in the Java utility.

```
keytool –import –alias root –keystore
        "install_directory\app-server\conf\security\jssecacerts" \
        –trustcacerts –file <filename_of_the_root_certificate>
```

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

```
keytool –importcert –alias dunes –keypass "dunesdunes" –file
         vcoCertificate.crt –keystore
         "install_directory\app-server\conf\security\jssecacerts" –storepass "dunesdunes"
```

The SSL certificate is installed. You can change the SSL certificate for the Orchestrator configuration interface or the SSL certificate for the Orchestrator client.

Adding the Certificate to the Local Store

After you get a certificate from a CA or create a certificate that matches your Orchestrator server name, you must add the certificate to your local store so that you can work with the Orchestrator configuration interface without receiving certificate warnings or error messages.

This workflow describes the process to add the certificate to your local store in Internet Explorer.

1 Open your Internet Explorer and navigate to https://*orchestrator_server_IP_or_DNS_name*:8283/.

2 When prompted, click **Continue to this website (not recommended)**.

   In Internet Explorer you see the Certificate Error on the right within the address bar.

3 Click the Certificate Error and select **View Certificates**.

4 Click **Install Certificate**.

5 On the Welcome page of the Certificate Import Wizard, click **Next**.

6 In the Certificate Store window, select **Place all certificates in the following store**.

7 Browse and select **Trusted Root Certification Authorities**.

8 Complete the wizard and restart Internet Explorer.

9 Navigate to the Orchestrator server over your SSL connection.

You no longer receive warnings and you do not receive a Certificate Error on the right within the address bar.

Other applications and systems (such as VMware Service Manager) must have access to the Orchestrator REST APIs over SSL connection.

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.

Back Up the Orchestrator Configuration and Elements

You can take a snapshot of your Orchestrator configuration and import this configuration into a new Orchestrator instance to back up your Orchestrator configuration. You can also back up the Orchestrator elements that you modified.

If you edit any standard workflows, actions, policies, or configuration elements, and then import a package containing the same elements with a higher Orchestrator 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.

Each Orchestrator server instance has unique certificates, and each vCenter Server plug-in instance has a unique ID. The certificates and the unique ID define the identity of the Orchestrator server and the vCenter Server plug-in. If you do not export the Orchestrator configuration or back up the Orchestrator elements for backup purposes, make sure that you change these identifiers.

Procedure

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

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

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

Use the same password when you import the configuration.

4 Click **Export**.

5 Log in to the Orchestrator client application.

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

a Click the **Packages** view.

b Click the menu button in the title bar of the Packages list and select **Add package**.

c Name the new package and click **OK**.

The syntax for package names is *`domain.your_company.folder.package_name`*..

For example, `com.vmware.myfolder.mypackage`.

d Right-click the package and select **Edit**.

e On the **General** tab, add a description for the package.

f On the **Workflows** tab, add workflows to the package.

g (Optional) Add policy templates, actions, configuration elements, resource elements, and plug-ins to the package.

7 Export the package.

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

b Browse to select a location where you want to save the package and click **Open**.

c (Optional) Sign the package with a specific certificate.

d (Optional) Impose restrictions on the exported package.

e (Optional) To apply restrictions for the contents of the exported package, deselect the options as required.

Option	Description
Export version history	The version history of the package is not exported.
Export the values of the configuration settings	The attribute values of the configuration elements in the package are not exported.
Export global tags	The global tags in the package are not exported.

f Click **Save**.

8 Import the Orchestrator configuration to the new Orchestrator server instance.

a Log in to the Orchestrator configuration interface of the new Orchestrator instance as vmware.

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

c Type the password you used while exporting the configuration.

This step is not necessary if you have not specified a password.

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

e Choose whether to override the Orchestrator internal certificate and network settings.

Select the check box only to restore your Orchestrator configuration and the `.vmoconfig` file is the backup file of the same Orchestrator configuration.

f Click **Import**.

9 Import the exported package to the new Orchestrator instance.

a Log in to the Orchestrator client application of the new Orchestrator instance.

b From the drop-down menu in the Orchestrator client, select **Administer**.

c Click the **Packages** view.

d Right-click within the left pane and select **Import package**.

e Browse to select the package that you want to import and click **Open**.

Certificate information about the exporter appears.

f Review the package import details and select **Import** or **Import and trust provider**.

The Import package view appears. If the version of the imported package element is later than the version on the server, the system selects the element for import.

g Deselect the elements that you do not want to import.

For example, deselect custom elements for which later versions exist.

h (Optional) Deselect the **Import the values of the configuration settings** check box if you do not want to import the values of the configuration elements attributes from the package.

i From the drop-down menu, choose whether you want to import tags from the package.

Option	Description
Import tags but preserve existing values	Import tags from the package without overwriting existing tag values.
Import tags and overwrite existing values	Import tags from the package and overwrite their values.
Do not import tags	Do not import tags from the package.

j Click **Import selected elements**.

Orchestrator Server Fails to Start

The VMware vRealize Orchestrator Server service might fail to start when the RAM available is not enough for the JVM to start the server.

Problem

The server status appears as `Starting` in the configuration interface and it is not updated when you refresh the page. When you select **My Computer > Services and Applications > Services**, the server fails to start and you receive a timeout error.

Cause

The Orchestrator server might not start in the following circumstances:

- Orchestrator runs on a system with less than 4 GB of RAM .
- The Orchestrator database runs on the same host as Orchestrator.
- Orchestrator is installed in a directory whose name contains non-ASCII characters.

Solution

- If you installed Orchestrator standalone, verify that your system has at least 4 GB of RAM.
- Verify that the Orchestrator database is running on a dedicated server.
- Verify that the Orchestrator components are configured properly and that all of the status indicators in the configuration interface display a green circle.

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 location of the `passwd.properties` configuration file.

Option	Action
If you installed the standalone version of Orchestrator	Go to *`install_directory`*`\VMware\Orchestrator\configuration\conf\`.
If you deployed the Orchestrator Appliance	Go to `/etc/vco/configuration/`.

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

3 Delete the contents of the file.

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

```
vmware=SHA512WithSalt\:GZ5wTW6Ni5x7\:wNCp8I8zHv7GQItrKDRjAgKsddjD4GUZ6nrOYhuEl3D
+x4BT5Xs1KL8f/R2T3K2nYPzMwVTW9E9mmbvESAU3ww\=\=
```

5 Save the `passwd.properties` file.

If you are using the Orchestrator Appliance, you might need to set the ownership of the `passwd.properties` file by running the `chown vco.vco passwd.properties` command.

6 Restart the vRealize Orchestrator Configuration service.

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

- User name: **`vmware`**
- Password: **`vmware`**

10 Setting System Properties

You can set system properties to change the default Orchestrator behavior.

This chapter includes the following topics:

Disable Access to the Orchestrator Client By Nonadministrators

You can configure the Orchestrator server to deny access to the Orchestrator client to all users who are not members of the Orchestrator administrator group.

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

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

Procedure

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

Option	Action
If you installed the standalone version of Orchestrator	Go to *`install_directory`*`\VMware\Orchestrator\app-server\conf`.
If you downloaded and deployed the virtual appliance	Go to `/etc/vco/app-server/`.

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

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

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

4 Save the `vmo.properties` file.

5 Restart the Orchestrator server.

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

Disable Access to Workflows from Web Service Clients

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

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

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

Procedure

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

Option	Action
If you installed the standalone version of Orchestrator	Go to *install_directory*\VMware\Orchestrator\app-server\conf.
If you downloaded and deployed the virtual appliance	Go to /etc/vco/app-server/.

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

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

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

4 Save the `vmo.properties` file.

5 Restart the Orchestrator server.

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

Setting Server File System Access for Workflows and JavaScript

Orchestrator limits access to the server file system from workflows and JavaScript to specific directories. You can extend access to other parts of the server file system by modifying the `js-io-rights.conf` Orchestrator configuration file.

The `js-io-rights.conf` file is created when a workflow tries to access the Orchestrator server file system. If the `js-io-rights.conf` file does not exist on your system, you can create it manually with the default content. For more information, see "Manually Create the js-io-rights.conf File on Windows Systems," on page 117.

Rules in the js-io-rights.conf File Permitting Write Access to the Orchestrator System

The `js-io-rights.conf` file contains rules that permit write access to defined directories in the server file system.

Mandatory Content of the js-io-rights.conf File

Each line of the `js-io-rights.conf` file must contain the following information.

- A plus (`+`) or minus (`-`) sign to indicate whether rights are permitted or denied
- The read (`r`), write (`w`), and execute (`x`) levels of rights
- The path on which to apply the rights

Default Content of the js-io-rights.conf File

The default content of the `js-io-rights.conf` configuration file in the Orchestrator Appliance is as follows:

```
-rwx /
+rwx /var/run/vco
-rwx /etc/vco/app-server/security/
+rx /etc/vco
+rx /var/log/vco/
```

The first two lines in the default `js-io-rights.conf` configuration file allow the following access rights:

`-rwx /`	All access to the file system is denied.
`+rwx /var/run/vco`	Read, write, and execute access is permitted in the `/var/run/vco` directory.

Rules in the js-io-rights.conf File

Orchestrator resolves access rights in the order they appear in the `js-io-rights.conf` file. Each line can override the previous lines.

The default configuration allows workflows and the Orchestrator API to write to the `c:/orchestrator` directory, but nowhere else.

IMPORTANT You can permit access to all parts of the file system by setting `+rwx /` in the `js-io-rights.conf` file. However, doing so represents a high security risk.

Set Server File System Access for Workflows and JavaScript

To change the parts of the server file system that workflows and the Orchestrator API can access, modify the `js-io-rights.conf` configuration file. The `js-io-rights.conf` file is created when a workflow attempts to access the Orchestrator server file system.

If the `js-io-rights.conf` file does not exist on your Windows system, you can manually create it with the default contents. You can create manually the file only on Windows systems. For more information, see "Manually Create the js-io-rights.conf File on Windows Systems," on page 117.

Orchestrator has read, write, and execute rights to a folder named `orchestrator`, at the root of the server system.

NOTE To locate the `js-io-rights.conf` on the Orchestrator Appliance, log in to the Orchestrator Appliance Linux console as root and navigate to the `/etc/vco/app-server` directory.

Procedure

1 Create the `c:/orchestrator` folder at the root of the Orchestrator server system.

2 Navigate to the folder that contains configuration files on the Orchestrator server system.

3 Open the `js-io-rights.conf` configuration file in a text editor.

4 Add the necessary lines to the `js-io-rights.conf` file to allow or deny access to parts of the file system.

For example, the following line denies the execution rights in the `c:/orchestrator/noexec` directory:

```
-x c:/orchestrator/noexec
```

`c:/orchestrator/exec` retains execution rights, but `c:/orchestrator/noexec/bar` does not. Both directories remain readable and writable.

You modified the access rights to the file system from workflows and from the Orchestrator API.

Create and Locate the js-io-rights.conf File in the Orchestrator Appliance

The `js-io-rights.conf` file is created when a workflow tries to access the Orchestrator server file system. You cannot create the `js-io-rights.conf` file manually in an Orchestrator Appliance instance.

Run a workflow that accesses the Orchestrator server file system and locate the `js-io-rights.conf` file to verify its existence.

Procedure

1 Log in to the Orchestrator client as an administrator.

2 Click the **Workflows** view.

3 In the workflows hierarchical list, select **Library > Troubleshooting**.

4 Right-click the **Export logs and application settings** workflow and select **Start workflow**.

NOTE This is an example workflow that tries to access the Orchestrator server file system.

5 Click **Submit**.

The `js-io-rights.conf` file is created.

6 Log in to the Orchestrator Appliance Linux console as **`root`** and navigate to the `/etc/vco/app-server/` directory.

7 Locate the `js-io-rights.conf` file.

8 (Optional) Verify the default content of the `js-io-rights.conf` file.

```
-rwx /
+rwx /var/run/vco
-rwx /etc/vco/app-server/security/
+rx /etc/vco
+rx /var/log/vco/
```

Manually Create the js-io-rights.conf File on Windows Systems

You can extend access to other parts of the Orchestrator server file system by modifying the `js-io-rights.conf` Orchestrator configuration file. If the `js-io-rights.conf` file does not exist on your Windows system, you can create it manually with the default content.

IMPORTANT You can create the `js-io-rights.conf` file only on Windows systems. The recommended way to generate the `js-io-rights.conf` file is to run a workflow that attempts to access the Orchestrator server file system. For information about creating the `js-io-rights.conf` file in the Orchestrator Appliance, see "Create and Locate the js-io-rights.conf File in the Orchestrator Appliance," on page 116.

Procedure

1 Log in as an administrator to the machine on which the Orchestrator server is installed.

2 Navigate to the Orchestrator configuration directory, located at *install_directory*`\VMware\Orchestrator\app-server\conf`.

3 Create the `js-io-rights.conf` file and open it in a text editor.

4 Type the default contents of the `js-io-rights.conf` file.

```
-rwx C:/

+rwx C:/orchestrator
# relative to user.dir which is %orchestrator_install_dir%\app-server\bin
+rx ../../app-server/logs/
+rx ../../configuration/logs/
+rx ../bin/
-rwx ../../app-server/conf/security/
+rx ../../app-server/conf/
+rx ../../apps/
+r ../../version.txt
```

5 Save and close the file.

You can now set the access to the server file system for workflows and JavaScript.

Set JavaScript Access to Operating System Commands

The Orchestrator API provides a scripting class, `Command`, that runs commands in the Orchestrator server host operating system. To prevent unauthorized access to the Orchestrator server host, by default, Orchestrator applications do not have permission to run the `Command` class. If Orchestrator applications require permission to run commands on the host operating system, you can activate the `Command` scripting class.

You grant permission to use the `Command` class by setting a system property in the `vmo.properties` properties file.

Procedure

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

Option	Action
If you installed the standalone version of Orchestrator	Go to *install_directory*`\VMware\Orchestrator\app-server\conf`.
If you downloaded and deployed the virtual appliance	Go to `/etc/vco/app-server/`.

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

3 Set the com.vmware.js.allow-local-process system property by adding the following line to the vmo.properties file.

```
com.vmware.js.allow-local-process=true
```

4 Save the vmo.properties file.

5 Restart the Orchestrator server.

You granted permissions to Orchestrator applications to run local commands in the Orchestrator server host operating system.

NOTE By setting the com.vmware.js.allow-local-process system property to true, you allow the Command scripting class to write anywhere in the file system. This property overrides any file system access permissions that you set in the js-io-rights.conf file for the Command scripting class only. The file system access permissions that you set in the js-io-rights.conf file still apply to all scripting classes other than Command.

Set JavaScript Access to Java Classes

By default, Orchestrator restricts JavaScript access to a limited set of Java classes. If you require JavaScript access to a wider range of Java classes, you must set an Orchestrator system property to allow this access.

Allowing the JavaScript engine full access to the Java virtual machine (JVM) presents potential security issues. Malformed or malicious scripts might have access to all of the system components to which the user who runs the Orchestrator server has access. Consequently, by default the Orchestrator JavaScript engine can access only the classes in the java.util.* package.

If you require JavaScript access to classes outside of the java.util.* package, you can list in a configuration file the Java packages to which to allow JavaScript access. You then set the com.vmware.scripting.rhino-class-shutter-file system property to point to this file.

Procedure

1 Create a text configuration file to store the list of Java packages to which to allow JavaScript access.

For example, to allow JavaScript access to all the classes in the java.net package and to the java.lang.Object class, you add the following content to the file.

```
java.net.*
java.lang.Object
```

2 Save the configuration file with an appropriate name and in an appropriate place.

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

Option	Action
If you installed the standalone version of Orchestrator	Go to *install_directory*\VMware\Orchestrator\app-server\conf.
If you downloaded and deployed the virtual appliance	Go to /etc/vco/app-server/.

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

5 Set the com.vmware.scripting.rhino-class-shutter-file system property by adding the following line to the vmo.properties file.

```
com.vmware.scripting.rhino-class-shutter-file=path_to_your_configuration_file
```

6 Save the vmo.properties file.

7 Restart the Orchestrator server.

The JavaScript engine has access to the Java classes that you specified.

Set Custom Timeout Property

When vCenter is overloaded, it takes more time to return the response to the Orchestrator server than the 20000 milliseconds set by default. To prevent this situation, you must modify the Orchestrator configuration file to increase the default timeout period.

If the default timeout period expires before the completion of certain operations, the Orchestrator server log contains errors.

```
Operation 'getPropertyContent' total time : '5742228' for 1823 calls, mean time : '3149.0', min time : '0', max time : '32313'
```

```
Timeout, unable to get property 'info' com.vmware.vmo.plugin.vi4.model.TimeoutException
```

Procedure

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

Option	Action
If you installed the standalone version of Orchestrator	Go to *install_directory*\VMware\Orchestrator\app-server\conf.
If you downloaded and deployed the virtual appliance	Go to /etc/vco/app-server/.

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

3 Set the com.vmware.vmo.plugin.vi4.waitUpdatesTimeout system property by adding the following line to the vmo.properties file.

```
com.vmware.vmo.plugin.vi4.waitUpdatesTimeout=<milliseconds>
```

4 Save the vmo.properties file.

5 Restart the Orchestrator server.

The value you set overrides the default timeout setting of 20000 milliseconds.

Modify the Number of Objects a Plug-In Search Obtains

By default, using the Orchestrator client to search for objects through a plug-in returns 20 objects at a time. You can modify the plug-in configuration file to increase the number of objects that are returned.

Prerequisites

You must have installed a plug-in in the Orchestrator server.

Procedure

1 Navigate to the plug-in configuration folder *install_directory*\VMware\Orchestrator\app-server\conf\plugins on the Orchestrator server system.

This folder contains an XML configuration file for each plug-in you have installed in the Orchestrator server.

2 Open the XML configuration file of the plug-in for which you want to change the number of search results.

3 Add the following line to the XML configuration file for the plug-in.

```
<entry key="ch.dunes.database.fetch-limit">50</entry>
```

This line sets the number of search results to return to 50.

4 Save the XML configuration file.

5 (Optional) Repeat Step 2 through Step 4 for each plug-in to modify.

6 Restart the Orchestrator server.

You increased the number of search results Orchestrator displays for a particular plug-in.

Modify the Number of Concurrent and Pending Workflows

By default, Orchestrator permits 300 workflows to run at the same time. When the Orchestrator server has to run more than 300 concurrent workflows, the pending workflow runs are queued. When an active workflow run completes, the next workflow in the queue starts to run. If the maximum number of queued workflows is reached, the next workflow runs fail until one of the pending workflows starts to run.

By setting system properties in the Orchestrator `vmo.properties` configuration file, you can control the number of workflows that are running at the same time and the number of pending workflows that are waiting in a queue.

IMPORTANT If your system is configured with one CPU, the recommended maximum value of the `com.vmware.vco.workflow-engine.executors-count` property is **`100`**. If the number of concurrent workflows is higher than 100, you might reach the maximum number of threads per processor.

Procedure

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

Option	Action
If you installed the standalone version of Orchestrator	Go to *`install_directory`*`\VMware\Orchestrator\app-server\conf`.
If you downloaded and deployed the virtual appliance	Go to `/etc/vco/app-server/`.

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

3 Set the `com.vmware.vco.workflow-engine.executors-count` and `com.vmware.vco.workflow-engine.executors-max-queue-size` properties by adding the following lines to the `vmo.properies` file.

```
com.vmware.vco.workflow-engine.executors-count=200
com.vmware.vco.workflow-engine.executors-max-queue-size=5000
```

4 Save the `vmo.properties` file.

5 Restart the Orchestrator server.

You set the maximum values for concurrent and pending workflows. You can run up to 200 workflows and 5000 workflows can be queued if the number of actively running workflows is reached.

11 Where to Go From Here

When you have installed and configured vRealize 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.
- Duplicate and modify the standard Orchestrator workflows and write your own actions and workflows to automate operations in vCenter Server.
- Develop plug-ins and Web services to extend the Orchestrator platform.
- Run workflows on your vSphere inventory objects by using the vSphere Web Client.

This chapter includes the following topics:

Log in to the Orchestrator Client on a Windows Machine

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 server machine and the Orchestrator client machine are synchronized.

Prerequisites

- All components of the Orchestrator server must be configured and the Orchestrator server service must be running.
- The Orchestrator client supports Java SE 7 and later.

Procedure

1. Log in as an administrator to the machine on which the Orchestrator client is installed.
2. Click **Start > Programs > VMware > vRealize Orchestrator Client**.
3. In the **Host name** field, type the IP address to which Orchestrator server is bound.

   To check the IP address, log in to the Orchestrator configuration interface and check the IP settings on the **Network** tab.

4 Log in by using the Orchestrator user name and password.

The default Orchestrator database (embedded database) and LDAP (embedded LDAP) settings are not suitable for a production environment.

Preconfigured Software	User Group (if any) and User	Password
Embedded Database	User: vmware	vmware
Embedded LDAP	User group: vcoadmins User: vcoadmin By default the vcoadmin user is set up as an Orchestrator administrator.	vcoadmin

To use Orchestrator in a production deployment, you must set up a separate database instance, set up an LDAP or vCenter Single Sign-On server, and configure Orchestrator to work with them.

NOTE LDAP authentication is deprecated.

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. Because of this, you receive a certificate warning each time you connect to the Orchestrator server.

Option	Description
Ignore	Click **Ignore** to 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.
Cancel	Click **Cancel** to close the window and stop the login process.
Install this certificate and do not display any security warnings for it anymore.	Select this check box and click **Ignore** to install the certificate and stop receiving security warnings.

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

The **My Orchestrator** view appears. This view summarizes the recent activities on the server, shows pending and running workflows, running policies, scheduled tasks, completed workflows, and elements you recently edited.

Log In to the Orchestrator Client from the Orchestrator Appliance Web Console

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.
- Verify that the appliance is up and running.

Procedure

1 In a Web browser, go to the IP address of your Orchestrator Appliance virtual machine.

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.

Option	Description
Ignore	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.
Cancel	Close the window and stop the login process.
Install this certificate and do not display any security warnings for it anymore.	Select this check box and click **Ignore** to install the certificate and stop receiving security warnings.

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 vRealize 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 vRealize Orchestrator*.

Index

W