vCenter Orchestrator Installation and Configuration Guide

vCenter Orchestrator 4.0

EN-000192-01

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

Updated Information

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

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

Revision	Description
EN-000192-01	■ Removed OpenLDAP from the list of supported directory services in "Supported Directory Services," on page 14. ■ Added information about unsupported database types and full partition warning in Chapter 6, "Orchestrator Database Setup," on page 21. ■ Added a note about an unsupported directory service type in Step 3 in "Generate the LDAP Connection URL," on page 27. ■ Added information about the methods Orchestrator uses to store passwords in "Password Encryption and Hashing Mechanism," on page 31. ■ Added instructions on how to remove a self-signed server certificate in "Change a Self-Signed Server Certificate," on page 34.
EN-000192-00	Initial release.

About This Book

The *VMware vCenter Orchestrator 4.0 Installation and Configuration Guide* provides information and instructions about installing, upgrading and configuring VMware® vCenter Orchestrator.

Intended Audience

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

Document Feedback

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

Technical Support and Education Resources

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

Online and Telephone Support

To use online support to submit technical support requests, view your product and contract information, and register your products, go to http://www.vmware.com/support.

Customers with appropriate support contracts should use telephone support for the fastest response on priority 1 issues. Go to http://www.vmware.com/support/phone_support.html.

Support Offerings

To find out how VMware support offerings can help meet your business needs, go to http://www.vmware.com/support/services.

VMware Professional Services

VMware Education Services courses offer extensive hands-on labs, case study examples, and course materials designed to be used as on-the-job reference tools. Courses are available onsite, in the classroom, and live online. For onsite pilot programs and implementation best practices, VMware Consulting Services provides offerings to help you assess, plan, build, and manage your virtual environment. To access information about education classes, certification programs, and consulting services, go to http://www.vmware.com/services.

Introduction to VMware vCenter Orchestrator 1

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

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 preexisting processes. Orchestrator is an open platform that can be extended with new plug-ins and libraries, and can be integrated into larger SOAP architectures through a set of APIs.

The following list presents the key Orchestrator features.

Persistence Production grade external databases are used to store relevant information, such as processes, 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 process 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 one of the following methods to create a step-by-step automation:

- Building blocks of the library
- Building blocks provided by the customer
- Plug-ins

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

Policy engine

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

Web 2.0 front end

The Web 2.0 front end allows new possibilities of expression and flexibility. It provides a library of user customizable components to access vCO orchestrated objects and uses Ajax technology to dynamically update content without reloading complete pages.

Security

Orchestrator provides the following advanced security functions:

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

Orchestrator User Roles and Related Tasks

vCenter Orchestrator provides different tools and interfaces based on the specific responsibilities of the three global user roles: Administrators, Developers, and End Users.

Administrators

This role has full access to all of the Orchestrator platform capabilities. Basic administrative tasks include the following items:

- Installing and configuring Orchestrator
- Managing access rights for Orchestrator and applications
- Importing and exporting packages
- Enabling and disabling Web views

- Running workflows and scheduling tasks
- Managing version control of imported elements

Developers

Users in this role 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
- Customizing Web front ends for these processes, using Web 2.0 technologies

End Users

Users in this role are granted access to only the Web front end. They can run and schedule workflows and policies.

Orchestrator Architecture

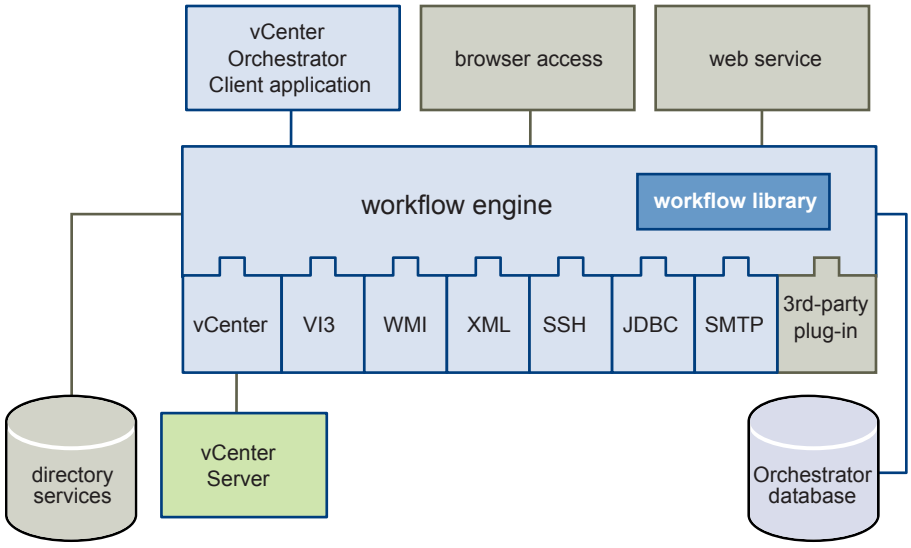
Orchestrator contains a workflow library and workflow engine to allow you to create and run workflows that automate orchestration processes. You run workflows on the objects of different technologies that Orchestrator accesses through a series of plug-ins.

Orchestrator provides a standard set of plug-ins, including a plug-in to VMware vCenter Server 4.0, to allow you to orchestrate tasks in the different environments that the plug-ins expose.

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

Figure 1-1 shows the architecture of Orchestrator.

Figure 1-1. VMware vCenter Orchestrator Architecture



Orchestrator System Requirements 2

This chapter describes the technical requirements that are necessary to install and configure VMware vCenter Orchestrator.

This chapter includes the following topics:

Hardware Requirements for Orchestrator

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

- 2.0GHz or faster Intel or AMD x86 processor. Processor requirements might differ if your database runs on the same hardware.
- 2GB RAM. You might need more RAM if your database runs on the same hardware.
- 10GB disk space. You might need more storage if your database runs on the same hardware.
- A free static IP address.

Operating Systems Supported by Orchestrator

Orchestrator offers support for several operating systems.

- Windows Server 2003 R2, 32bit
- Windows Server 2003 R2, 64bit
- Windows Server 2008, 32bit
- Windows Server 2008, 64bit

Supported Directory Services

Orchestrator requires a working LDAP server on your infrastructure.

The supported directory service types are:

- Active Directory
- eDirectory
- Sun Java Directory Server

Browsers Supported by Orchestrator

The Orchestrator user interface requires a Web browser.

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

- Microsoft Internet Explorer 6.0 and 7.0
- Mozilla Firefox 3.0.6 or later
- Safari 3.x (experimental)

Orchestrator Database Requirements

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

NOTE Because of CPU and memory use, VMware recommends that you host the Orchestrator database and the Orchestrator server on different machines from the same datacenter.

The following database types are supported by Orchestrator:

- Microsoft SQL Server 2005 Enterprise (SP2)
- Microsoft SQL Server 2005 Enterprise (SP2) x64
- Microsoft SQL Server 2005 Enterprise (SP1)
- Microsoft SQL Server 2005 Standard (SP2)
- Microsoft SQL Server 2005 Standard (SP1)
- Microsoft SQL Server 2000 Enterprise (SP4)
- Microsoft SQL Server 2000 Standard (SP4)
- Oracle 10g Enterprise Release 2 (10.2.0.3.0) x64
- Oracle 10g Enterprise Release 2 (10.2.0.3.0) x32

Installing Orchestrator with vCenter Server

3

When you install VMware vCenter Server, Orchestrator (client and server) is silently installed on your system as an additional component. To make it available for use, you must configure it.

NOTE Orchestrator does not support IPv6 operating systems. You can only configure it using IPv4.

If you have an installation of Orchestrator 3.0.1 and are planning to install Orchestrator 4.0 with the vCenter Server installer, make sure that the VMware vCenter Orchestrator Configuration Service is stopped before you proceed.

For detailed instructions about vCenter Server installation, see the *ESX and vCenter Server Installation Guide*.

Install Orchestrator Standalone on Microsoft Windows

4

If you install VMware vCenter Server, Orchestrator (client and server) is already installed on your system and to make it available for use, you must configure it. If vCenter Server is not installed on your Windows server, you can install Orchestrator as a standalone product.

Prerequisites

Make sure that your hardware meets the Orchestrator system requirements. See "Hardware Requirements for Orchestrator," on page 13.

Procedure

1 Download the `vCenterOrchestrator.exe` file.

2 Double-click the `.exe` file and click **Next**.

The installation process begins.

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

4 Select the installation directory and click **Next**.

- If you install the standalone version of Orchestrator the default location is `C:\Program Files\VMware\Orchestrator`.
- If you install the standalone version of Orchestrator on Windows Server 2008, 64bit, the default location is `C:\Program Files(x86)\VMware\Orchestrator`.
- If the vCenter Server installer installed Orchestrator the default location is `C:\Program Files\VMware\Infrastructure\Orchestrator`.

To install to a different location, click **Choose** and browse for the new location.

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

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

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

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

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

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

What to do next

Log in to the Orchestrator Configuration interface form **Start > Programs > VMware > vCenter Orchestrator Web Configuration** and change the default password.

Upgrading Orchestrator Applications After Upgrading vCenter Server

5

If you upgrade the virtual infrastructure from VMware Infrastructure 3.5 to vCenter Server 4.0, you must take action to continue to run your existing applications.

One course of action is to install the VMware Infrastructure 3.5 plug-in on an Orchestrator server 4.0 platform and then import your applications. The VMware Infrastructure 3.5 plug-in communicates with the vCenter Server 4.0 plug-in and allows you to run your applications without change.

Alternatively, to benefit from all the features of vCenter Server 4.0, you can refactor Orchestrator applications that you wrote with the old version. Orchestrator 4.0 provides workflows to help you refactor the applications to the new version.

For detailed information about refactoring applications, see *vCenter Orchestrator Developer's Guide*.

Orchestrator Database Setup 6

Orchestrator requires a database to store information about workflows, users, roles, and permissions.

Orchestrator server fully supports Oracle and SQL Server databases and provides experimental support for MySQL and PostgreSQL. You can use MySQL and PostgreSQL for testing and evaluation purposes.

NOTE The driver for MySQL is not installed together with Orchestrator. For details about enabling support for this database type, see "Enable Support for MySQL Databases on Windows," on page 21.

The way in which your database is set up can affect Orchestrator performance. Install the database in a virtual machine other than the one on which Orchestrator is installed. This method avoids the JVM and DB server having to share CPU, RAM, and IOs. Storing your database plug-ins in a database separate from the one used by Orchestrator allows more modularity when upgrading the system.

CAUTION Ensure at least 1GB of free disk space on the virtual machines where the database and Orchestrator servers are installed. Insufficient disk storage space might result in unwanted behavior of the Orchestrator server and client.

This chapter includes the following topics:

Enable Support for MySQL Databases on Windows

To use a MySQL database, you must download the driver and copy it to the appropriate locations. The Orchestrator installer does not install drivers for MySQL databases.

Procedure

1 Download the latest MySQL driver from the MySQL drivers Web page.

The download you need is under the *MySQL Connector/J - for connecting to MySQL from Java* heading.

2 Extract the downloaded archive.

3 In the extracted folder, locate the `mysql-connector-java-<x.x.x>.jar` file, where <x.x.x> is the current subminor version.

4 To make the driver available to VMware vCenter Orchestrator server and VMware vCenter Orchestrator configuration interface, copy `mysql-connector-java-<x.x.x>.jar` to the following locations:

   - VMware vCenter Orchestrator configuration interface:

     `C:\Program Files\VMware\Orchestrator\configuration\jetty\lib\ext\`

   - VMware vCenter Orchestrator server:

     `C:\Program Files\VMware\Orchestrator\app-server\server\vmo\lib\`

5 Restart the Orchestrator servers.

   a Right-click **My Computer** on your desktop and select **Manage**.

   b In the Computer Management dialog box, expand **Services and Applications** and select **Services**.

   c In the right pane, right-click and select **VMware vCenter Orchestrator Server > Restart** .

   d In the right pane, right-click and select **VMware vCenter Orchestrator Configuration > Restart** .

The MySQL database driver is installed.

MySQL Database Parameters

When you use a MySQL database, the database server must be configured with the parameter `max_allowed_packet` set to 16M.

Procedure

1 On Windows, edit the following file: `C:\Program Files\MySQL\MySQL Server <X.X>\my.ini`.

2 In section [mysql], add the following line: **`max_allowed_packet = 16M`**.

Configuring Orchestrator 7

VMware vCenter Orchestrator Web Configuration is installed silently with VMware vCenter Server. This is the tool you use to configure the components that are related to the Orchestrator engine, such as network, database, server certificate, and so on. The correct configuration of these components ensures the proper functioning of Lifecycle Manager or any other applications running on the Orchestrator platform.

This chapter includes the following topics:

Start the Orchestrator Configuration Service

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

If you installed Orchestrator using GUI or console mode, the Web configuration service is already started.

Procedure

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

2 Locate VMware vCenter Orchestrator Configuration on the list and check its status.

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

The 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

Make sure that the VMware vCenter Orchestrator Configuration service is running.

Procedure

1 To access the Orchestrator configuration interface, do one of the following:

- Select **Start > Programs > VMware > vCenter Orchestrator Web Configuration** .
- Open a Web browser window and enter the following URL:

  `http://<computer_DNS_name_or_IP_address>:8282`.

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

2 Log in with the default credentials:

- User name: **`vmware`**
- Password: **`vmware`**

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

For more details about changing the default password, see "Change the Default Password," on page 25.

You cannot change the **`vmware`** default user name.

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

What to do next

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

Change the Default Password

VMware recommends that you change the default password to avoid potential security issues.

Prerequisites

Make sure that the VMware vCenter 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 **vmware**.

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

5 Reenter the new password to confirm it.

6 Click **Apply changes** to save the new password.

Configure the Network Connection

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

Prerequisites

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

Procedure

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

2 Click **Network**.

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

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

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

4 Set up the communication ports.

For more information about default ports, see "Default Configuration Ports," on page 26.

5 Click **Apply changes**.

What to do next

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

Default Configuration Ports

Orchestrator uses some specific ports that allow communication with the other systems. It is embedded in a JBoss application server, and benefits from built-in redundancy, high-availability, high-performance distributed application services and support for complex database access.

The communication ports you must set are a subset of the standard ports used by JBoss. The ports are set with a default value, but you can change these values at any time. When you make the changes, ensure that all ports are free on your host and, if necessary, open these ports on required firewalls.

For a list of default ports, see Table 7-1.

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

Table 7-1. VMware vCenter Orchestrator Default Ports

Communication Port	Port Number	Description
Lookup port	8230	The main port to communicate with the Orchestrator server (JNDI port). All other ports communicate with the Orchestrator smart client through this port. It is part of the Jboss Application server infrastructure.
Command port	8240	The application communication port (RMI container port) used for remote invocations. It is part of the Jboss Application server infrastructure.
Messaging port	8250	The Java messaging port used to dispatch events. It is part of the Jboss Application server infrastructure.
Data port	8244	The port used to access all Orchestrator data models, such as workflows and policies. It is part of the Jboss Application server infrastructure.
HTTP server port	8280	The port for the HTTP connector used to connect to the Web front-end.
HTTPS server port	8281	The SSL secured HTTP protocol used to connect to the Web front-end and to communicate with vCenter API.
Web configuration HTTP access port	8282	The access port for the Web UI of Orchestrator configuration.
Web configuration HTTPS access port	8283	The SSL access port for the Web UI of Orchestrator configuration. **NOTE** To enable the HTTPS connection, configure Jetty to use SSL. For details, see *Jetty Documentation, Configuring SSL*.
LDAP	389	The look up port of your LDAP Authentication server.
LDAP using SSL	636	The look up port of your secure LDAP Authentication server.
PostgreSQL	5432	PostgreSQL Server for Orchestrator database.
SQL Server	1433	Microsoft SQL Server for Orchestrator database.
Oracle	1521	Oracle Database for Orchestrator database.
MySQL	3306	MySQL for Orchestrator database.
SMTP Server port	25	Used for email notifications.
vCenter API port	443	vCenter API communication port

Import the vCenter SSL Certificate

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

Procedure

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

2 Click **Network**.

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

4 To load the vCenter SSL certificate in Orchestrator, do one of the following:

Option	Description
Import from URL	Enter URL of the vCenter server: `https://<your_vcenter_server_IP_address>`
Import from file	Ensure that you are connected to the remote server and click **Browse** to search for the certificate file of a vCenter server you have saved on your machine. For example: `C:\Documents and Settings\AllUsers\ApplicationData\VMware \VMware VirtualCenter\SSL\rui.crt`. ESX hosts use a self-generated SSL certificate located in the following directory: `/etc/vmware/ssl/rui.crt`.

5 Click **Import**.

A message confirming that the import is successful appears.

6 Repeat Step 3 through Step 5 for each vCenter server.

7 Click **Start-up Options**.

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

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

What to do next

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

Configuring LDAP Settings

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

Generate the LDAP Connection URL

When you generate the LDAP look up URL you must specify the LDAP host, port, and root.

Procedure

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

2 Click **LDAP**.

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

The supported directory service types are: Active Directory, eDirectory, and Sun Java System Directory Server. OpenLDAP is not supported and can only be used for testing and evaluation purposes.

NOTE If you change the LDAP server or type after you set permissions on Orchestrator objects (such as access rights on workflows or actions), you must reset these permissions.

If you change the LDAP settings after configuring custom applications that capture and store user information, the LDAP authentication records created in the database become invalid when used against the new LDAP database.

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

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

5 In the **Primary LDAP Host** text box, enter 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, enter 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, enter the value for the look up port of your LDAP server.

NOTE Orchestrator supports Active Directory hierarchical domains structure. You can use the default port 389 to connect to the Global Catalog server.

If your Domain Controller is not configured to use Global Catalog, you must use port 3268.

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

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

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

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

NOTE SSL capabilities are not installed as part of Microsoft Active Directory, eDirectory and Sun Java Directory Server, and might require additional configuration.

Example 7-1. Example Values and 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`

What to do next

Assign credentials to Orchestrator to ensure its access to the LDAP server.

For more details, see "Specify the Browsing Credentials," on page 29.

Specify the Browsing Credentials

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

Prerequisites

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

Procedure

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

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

- Bare user name format, for example **`user`**.
- Distinguished name format: **`cn=user,ou=employees,dc=company,dc=org`**.

  Use this format with OpenLDAP, Sun, and eDirectory.
- Principle name format: **`user@company.org`**.
- NetBEUI format: **`COMPANY\user`**.

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

Orchestrator uses these credentials to connect to the LDAP server.

What to do next

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

Define the LDAP Lookup Paths

You can define the users and groups lookup information.

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

Prerequisites

You must have a working LDAP service on your infrastructure.

Procedure

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

2 Click **LDAP**.

3 Define the **User lookup base**.

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

a Click **Search** and enter the top-level domain name.

Searching for **`company`** returns `dc=company,dc=org` and other common names containing the search term. If you enter **`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 389. It issues LDAP referrals which Orchestrator follows to find the account or group in a subdomain.

4 Define the **Group lookup base**.

This is the LDAP container where Orchestrator looks up groups.

a Click **Search** and enter the top-level domain name.

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

5 Define the **vCO Admin group**.

This is the LDAP group to whom you grant administrative privileges for Orchestrator.

a Click **Search** and enter the top-level domain name.

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

IMPORTANT In eDirectory installations, only the eDirectory administrator can see users or user groups that have administration rights. If you are using an eDirectory LDAP server, and you log into Orchestrator as a member of the vCO Admin group but you are not the eDirectory administrator, you can create users or user groups with administration rights, but you cannot see those users using their own rights and permissions. This issue does not apply to other LDAP servers.

What to do next

Click the **Test Login** tab and enter credentials for a user to test whether they can access the Orchestrator smart client. After a successful login, the system checks if the user is in the Orchestrator Administrator group.

Set Connection Timeouts

If your system is timing out, you can increase the timeout period on the Orchestrator client side and on the LDAP server side.

Increasing the clientside timeout period is pointless if the serverside timeout period remains shorter than the clientside. Increasing the serverside timeout period might not be advisable for other processes that rely on the enterprise LDAP server.

Procedure

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

2 Click **LDAP**.

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

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

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

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

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

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

6 (Optional) To disable referral handling, select the **Ignore referrals** check box.

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

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

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

8 Click **Apply changes**.

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

What to do next

Proceed with the database configuration.

Password Encryption and Hashing Mechanism

Orchestrator utilizes PBE with DES encryption and an MD5 hashing mechanism to ensure secure connections to the database, LDAP, and Orchestrator servers.

Table 7-2 shows the password encryption methods used by Orchestrator.

Table 7-2. Encryption and Hashing Algorithms

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

Configure the Database Connection

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

Prerequisites

Set up a database to use with the Orchestrator server. For more information, see Chapter 6, "Orchestrator Database Setup," on page 21.

Procedure

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

2 Click **Database**.

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

4 Specify the database connection parameters.

Connection Parameter	Description
Username	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, and must have table-creation and table-deletion rights.
Password	The password that Orchestrator accepts with the user name you select.
Hostname or IP	The database server IP address or DNS name.
Port	The database server port that allows communication to your database.
Database name	The full unique name of your database. The database name is specified by the `SERVICE_NAMES` parameter in the initialization parameter file. **NOTE** PostgreSQL JDBC driver does not support non-ASCII characters in the database name.
Instance name	The name of the database instance that can be identified by the `INSTANCE_NAME` parameter in the database initialization parameter file.
Domain	For Windows authentication, enter the Windows domain, for example **`company.org`**. For SQL authentication, leave this text box blank.

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 installation is not yet complete. You must install the database.

5 Click **Install database** to build the table structure for Orchestrator.

6 Click **Apply changes**.

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

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

Server Certificate

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

To acquire a server certificate, perform the following tasks:

1 Create a self-signed server certificate.

2 Generate a Certificate Signing Request (CSR).

3 Submit the CSR to a Certificate Authority (CA).

4 Import the Certificate Signing Reply.

Create a Self-Signed Server Certificate

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

Procedure

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

2 Click **Server Certificate**.

3 Click **Create a new Certificate Database and server certificate**.

4 Enter the relevant information.

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

6 Click **Create**.

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

What to do next

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

Obtain a Server Certificate Signed by a Certificate Authority

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

Prerequisites

Create a self-signed server certificate or click **Import vCO Certificate Database** to import an existing server certificate.

Procedure

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

2 Click **Server Certificate**.

3 Generate a Certificate Signing Request (CSR).

   a Click **Export Certificate Signing Request**.

   b Save the `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.

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

5 Click **Import Certificate Signing Reply** and select the file sent by your CA.

Orchestrator uses the server certificate to:

- Sign all packages before they are exported by attaching your certificate's public key to each one.
- Display a user prompt on importing a package that contains elements signed by untrusted certificates.

What to do next

You can import this certificate on other servers.

Export a Server Certificate

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

Prerequisites

You must have created or imported a server certificate.

Procedure

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

2 Click **Server Certificate**.

3 Click **Export vCO Certificate Database**.

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

You must enter this password again when importing the file.

5 Click **Export**.

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

Change a Self-Signed Server Certificate

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

Procedure

1 Export all your packages.

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

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

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

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

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

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

f Click **Save**.

2 (Optional) Export the Orchestrator configuration.

3 Uninstall the Orchestrator server.

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

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

5 Reinstall the Orchestrator server.

6 (Optional) Import your Orchestrator configuration.

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

8 Reimport your packages.

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

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

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

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

   e Click **Import checked elements**.

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

Configure the Default Plug-Ins

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

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

Procedure

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

2 Click **Plug-ins**.

3 Enter the credentials for a user who is a member of the Orchestrator Administration group.

   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 install a new plug-in:

   a Click **Browse**.

   b Select the file to install.

   c Click **Open**.

   d Click **Upload and install**.

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

   The installed plug-in file is stored in the `<Install_Directory>\app-server\server\vmo\plugins` folder.

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

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

   This action does not remove the plug-in file.

6 Click **Apply changes**.

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

What to do next

You can now configure the settings for Mail, SSH, and vCenter 4.0 plug-ins.

Define the Default SMTP Connection

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

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

Procedure

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

2 Click **Mail**.

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

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

4 Click **Apply changes**.

Configure the SSH Plug-In

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

Procedure

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

2 Click **SSH**.

3 Click **New connection**.

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

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

5 Click **Apply changes**.

The host is added to the list of SSH connections.

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

a Click **New root folder**.

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

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

Configure the vCenter 4.0 Plug-In

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

Prerequisites

Import the SSL certificates for each vCenter instance you define. For more information, see "Import the vCenter SSL Certificate," on page 27.

Procedure

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

2 Click **vCenter 4.0**.

3 Click **New vCenter host**.

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

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

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

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

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

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

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

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

10 Specify the method you use to manage user access on the vCenter host by selecting one of the following options:

Option	Description
Share a unique session	Enter the credentials of a user who is a vCenter administrator.
Session per user	Select this option if your vCenter server is in an Active Directory domain. Make sure that the user has the necessary permissions to perform the required operations. CAUTION Each user who logs in creates their own session to vCenter. This results in higher traffic and more inquiries.

11 Click **Apply changes**.

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

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

What to do next

If you did not restart the server after importing the vCenter SSL Certificate, click **Restart the vCO Configuration 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 7-3 describes the set of privileges on the Orchestrator server, depending on your vCenter Server license edition.

Table 7-3. Orchestrator Server Modes

vCenter License Edition	Orchestrator Server Mode	Description
Standard	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. You must duplicate the workflow and make changes to your own workflow.
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.

Import the vCenter Server License

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

Procedure

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

2 Click **Licenses**.

3 In the **Serial Number** text box, enter your vCenter Server license key.

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

4 Click **Apply changes** and verify that the license is installed.

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

5 Start the Orchestrator server.

The Orchestrator server is now configured correctly.

Start the Orchestrator Server

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

Prerequisites

Make sure that all of 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 Click **Install vCO server as service**.

4 Click **Start service**.

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

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

- Running
- Not available
- Stopped

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

What to do next

You can save and export the Orchestrator configuration file so that it can be imported later if needed. For more details, see "Export the Orchestrator Configuration," on page 40.

Activate the Service Watchdog

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

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

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

Prerequisites

You are running the Orchestrator server as a Windows service.

Procedure

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

You find the wrapper configuration file in the following location:

```
<Install_Directory>/app-server/bin/wrapper.conf
```

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

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

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

The default timeout is 0 seconds, meaning that the watchdog is deactivated. You increase the timeout period to 30 seconds as follows.

```
-wrapper.ping.timeout=30
```

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

6 Restart the Orchestrator server by clicking **Startup Options > Restart Service** in the Orchestrator configuration interface.

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

NOTE If the Orchestrator server is running with a heavy load, for example if you have connected Orchestrator to many vCenter Servers which are running many virtual machines, or if the server is performing swapping, you might experience unwanted server restarts if you have activated the watchdog. In certain circumstances, if the response time exceeds the watchdog timeout period, the watchdog can falsely detect a JVM error, which causes it to restart the server.

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

Export the Orchestrator Configuration

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

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

Procedure

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

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

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

Use the same password when you import the configuration.

4 Click **Export**.

5 Click **Save** when prompted.

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

What to do next

For a list of exported configuration settings, see "Orchestrator Configuration Files," on page 40.

Orchestrator Configuration Files

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

NOTE Some of the configuration files that are created during the export are empty. For example, the server file is empty because the startup options for the Orchestrator server are individual for each machine where the Orchestrator server is installed. These empty files must be reconfigured, even when a working configuration was previously imported.

Table 7-4 contains a list of the settings that are not saved during configuration export.

Table 7-4. Settings Not Saved During Configuration Export

File	Description
certificate	Certificates are not exported. Most certificates are stored in the Orchestrator database. However, the vCenter Server certificate is not stored in the database. You must store it in a separate location, or import it again when you import an Orchestrator configuration.
licenses	Licenses are not exported. They are stored in the Orchestrator database.
server	The server configuration.

Table 7-5 contains a list of the settings that are saved during configuration export.

Table 7-5. Settings Saved During Configuration Export

File	Description
general	The maximum number of completed events and workflows recorded, and the Web view development and configuration.
network	The IP binding address and the TCP ports used by the different elements of the Orchestrator server.
database	The database configuration.
ldap	The LDAP server configuration.
log	The log settings information.
plug-ins	The list of disabled plug-ins and the account name.
troubleshooting	Debugging information.
mail plug-in	The SMTP host, SMTP port, user name, password, sender's name, sender's address.
vCenter 4.0 plug-in	The vCenter 4.0 plug-in configuration.

Import the Orchestrator Configuration

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

Procedure

1 Install a new Orchestrator instance on a new server.

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

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

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

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

6 Click **Import**.

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

Configure the Maximum Number of Events and Executions

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

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

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

Procedure

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

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

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

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

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

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

5 (Optional) To set the default login credentials, fill in the **Web auto-login user name and password** text boxes.

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

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

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

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

In this mode, all elements in the Web view are loaded from the specified Web view directory and no longer from the Web view content itself.

8 Click **Apply changes**.

Install an Application

An application is a set of plug-ins and packages. Because a Orchestrator installation contains only a few pre-defined plug-ins, you must install applications frequently to extend basic functions.

Prerequisites

Obtain the `.vmoapp` file containing the application.

Procedure

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

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

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

4 Click **Install**.

What to do next

Every time you install an application, a validation is made on the server configuration. In most cases, you must perform additional configuration steps.

Start a Published Web View

You can use Web views to build the user front-end. Web views might vary from a simple page displaying basic information to complex Web 2.0 applications. Orchestrator provides a demonstration Web view called WebOperator, which you can use to review how Web views work. You can access Web views through the Orchestrator configuration interface.

Prerequisites

Make sure that the Orchestrator server is started.

Procedure

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

2 On the **General** tab, click **Web views**.

The links to your published Web views appear. You can follow them to open a Web view in a new browser window.

Start the weboperator Web View

Orchestrator provides a standard Web view called weboperator that allows users to run workflows from a browser.

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

NOTE The weboperator Web view provides access to all the objects in the inventory and all the workflows in the library to all users. To limit access to certain objects and certain workflows on a per-user basis, use the Perspectives Web view. For information about the Perspectives Web view, see the *vCenter Orchestrator Administration Guide*.

Procedure

1 Log into the Orchestrator client.

2 Click **Web Views**.

The weboperator Web view and any other Web views that you have imported into Orchestrator appear.

3 Right-click weboperator and select **Publish**.

4 Open a browser and go to `http://<orchestrator_server>:8280`.

In the URL, <orchestrator_server> is the DNS name or IP address of the Orchestrator server, and 8280 is the port number upon which Orchestrator publishes Web views.

5 In the Orchestrator home page, click **Web View List**.

6 Click **weboperator**.

7 Log in using your Orchestrator user name and password.

8 Expand the hierarchical list of workflows to navigate through the workflows in the Orchestrator library.

9 Click a workflow in the hierarchical list to display information about the workflow in the right pane.

10 In the right pane, select whether to run the workflow now or at a later time.

Option	Action
Run the workflow now	a Click **Execute Workflow** to run the workflow. b Provide the required input parameters and click **Submit** to run the workflow.
Run the workflow at a later time	a Click **Schedule Workflow** to run the workflow at a later time. b Provide the time, date, and recurrence information to set when and how often to run the workflow and click **Next**. c Provide the required input parameters and click **Submit** to schedule the workflow.

You can use the weboperator Web view to run workflows on objects in your inventory from a Web browser rather than from the Orchestrator client.

What to do next

If you only need a Web view to access the inventory and run workflows, then the standard weboperator and Perspectives Web views should meet your requirements. If you require more complex functionality from a Web view, you can use the Web components and Web view template that Orchestrator provides to develop custom Web views.

Define the Server Log Level

In the Orchestrator configuration interface, you can set the level of server log you require.

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 entries are written to the log file.
ERROR	Errors and above entries are written to the log file.
WARN	Warnings and above entries are written to the log file.
DEBUG	Debug information and above entries are written to the log file.
INFO	Information and above entries are written to the log file.
ALL	Events are not filtered. All event are written to the log file.
OFF	No entries are written to the log file and no log updates are made.

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

4 Click **Apply changes**.

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

This operation creates a ZIP archive of all logs.

The new server log level is applied within a minute without server restart. The logs are stored in `<Install directory>\app-server\server\vmo\log\`.

Index