VMware Identity Manager Connector Installation and Configuration (Legacy Mode)

VMware Identity Manager

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-001790-07

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

VMware Identity Manager Connector Installation and Configuration (Legacy Mode)

VMware Identity Manager Connector Installation and Configuration (Legacy Mode) explains how to install and configure the connector virtual appliance in legacy mode and set up the connection to your enterprise directory to sync users and groups to the directory in the VMware Identity Manager service. Legacy mode requires allowing inbound connections to the connector appliance installed on premises.

To install the VMware Identity Manager connector in outbound-only connection mode, see *VMware Identity Manager Cloud Deployment*.

Intended Audience

The information is written for experienced Windows and Linux system administrators who are familiar with VMware technologies, particularly vCenter™, ESX™, vSphere®, networking concepts, Active Directory servers, databases, backup and restore procedures, Simple Mail Transfer Protocol (SMTP), and NTP servers. SUSE Linux 11 is the underlying operating system for the virtual appliance.

Knowledge of other technologies, such as x509 digital certification, RSA SecurID, and Active Directory, is helpful if you plan to implement those features.

Preparing to Install VMware Identity Manager Connector

1

You deploy the VMware Identity Manager Connector virtual appliance OVA and use the Setup wizard to activate your connector with your tenant in the VMware Identity Manager service. After the connector is deployed, you log in to the administration console and configure your directory and set up authentication methods.

VMware vSphere Client or vSphere Web Client is required to deploy the OVA file and access the deployed virtual appliance remotely. The vSphere client application can be downloaded from the VMware vSphere product download page.

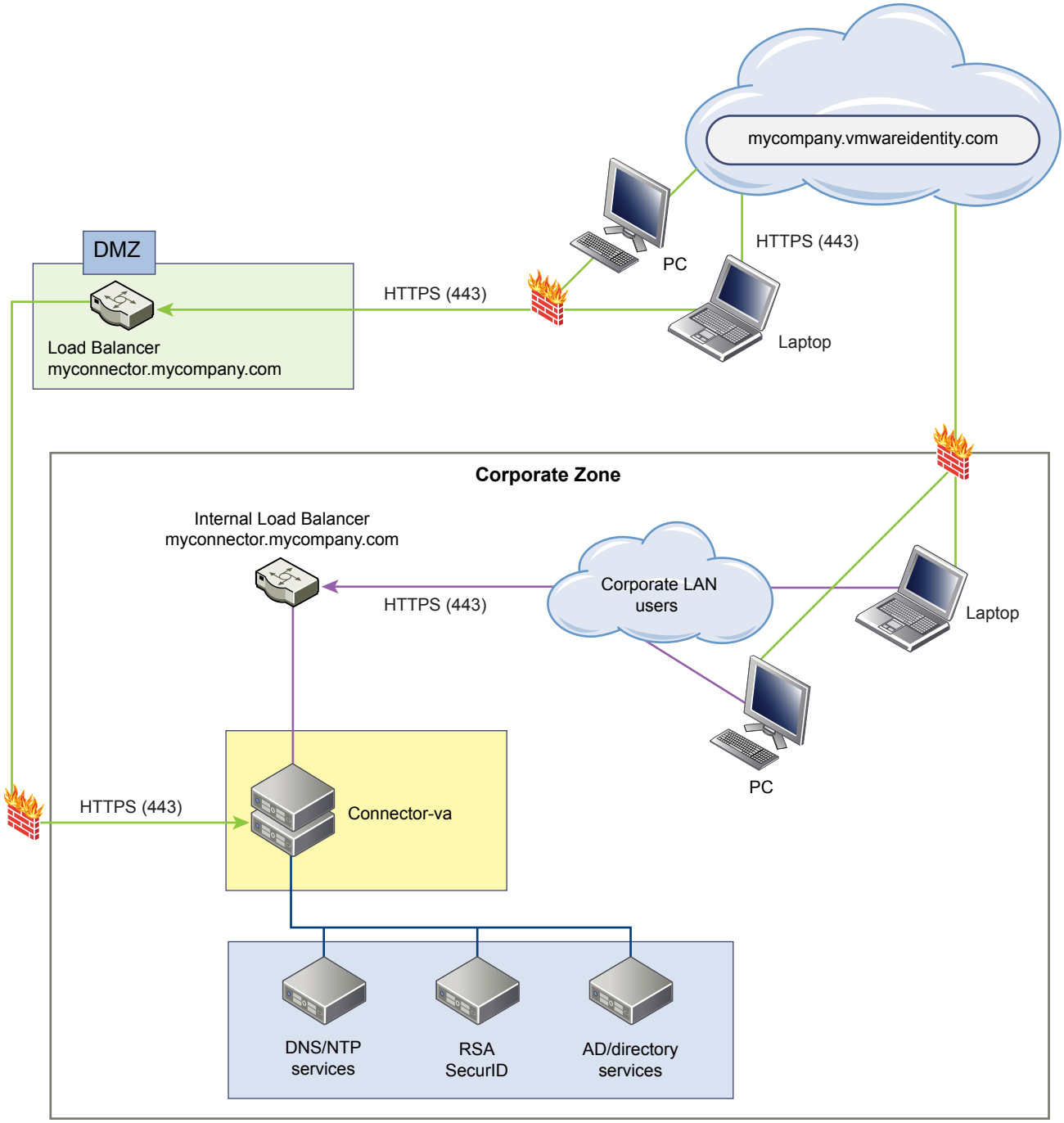
This chapter includes the following topics:

Planning the Deployment Strategy

The connector component of VMware Identity Manager is delivered as a virtual appliance that is deployed on site and integrates with your enterprise directory to sync users and groups to the VMware Identity Manager service and to provide authentication.

As you plan for your deployment, consider your organization's objectives. During the deployment, the connector is set up inside the internal network. Internal and external users who log in to the VMware Identity Manager service are redirected to the connector for authentication. You must install a load balancer in the DMZ to provide access to the connector from both inside the corporate network and from outside the firewall. You can install a load balancer, such as Apache, NGINX, or F5. See "Using a Load Balancer to Enable External Access to the Connector," on page 25.

Figure 1-1. Typical Connector Deployment with VMware Identity Manager



For redundancy and failover you add additional connector virtual appliances to form a cluster. If one appliance is unavailable, the connector is still available. All nodes in the cluster are identical and nearly stateless copies of each other. See Configuring Failover and Redundancy.

The connector is the initial identity provider to provide authentication. If your organization has specific authentication policies, you can integrate a third party identity provider to support the additional authentication methods. See the *VMware Identity Manager Administration Guide*.

General Configuration Requirements

Before you install the connector virtual appliance, plan how you want to set up your DNS records, connect to your enterprise directory, and authenticate users.

Prepare Your DNS Records and IP Addresses

A DNS entry and a static IP address must be available for the connector. Because each company administers their IP addresses and DNS records differently, before you begin to set up the connector, request the DNS record and IP addresses to use.

Directory Requirement

The VMware Identity Manager service uses your enterprise directory infrastructure for user authentication and management. You can integrate the service with an Active Directory environment that consists of a single Active Directory domain, multiple domains in a single Active Directory forest, or multiple domains across multiple Active Directory forests. You can also integrate the service with an LDAP directory.

Your directory must be accessible to the connector virtual appliance to sync users and groups. You configure the directory connection after you set up the connector. See Chapter 5, "Integrating with Your Enterprise Directory," on page 31, Chapter 6, "Integrating with Active Directory," on page 33, and Chapter 7, "Integrating with LDAP Directories," on page 47.

User Authentication Methods

The connector virtual appliance supports various authentication methods including passwords, Kerberos, RSA Secure ID, and Certificate user authentication. Users are authenticated based on the authentication methods you set up. For information about setting up user authentication, see the *VMware Identity Manager Administration Guide*.

System and Network Configuration Requirements

Consider your entire deployment, including how you integrate resources, when you make decisions about hardware, resources, and network requirements.

Supported vSphere and ESX Versions

The following versions of vSphere and ESX server are supported:

- 5.0 U2 and later
- 5.1 and later
- 5.5 and later
- 6.0 and later

Virtual Appliance Requirements

Ensure that the resources allocated to the connector virtual appliance meet the minimum requirements.

Component	Minimum Requirement
CPU	2
Random-access memory	6GB
Disk space	24GB

Network Configuration Requirements

Component	Minimum Requirement
DNS record and IP address	IP address and DNS record
Firewall port	Ensure that the inbound firewall port 443 is open for users outside the network to the connector instance or the load balancer. **Important** Make sure that the outbound firewall port 443 is open from the connector instance to the vmwareidentity.com URL.
Reverse Proxy	

Port Requirements

Ports used in the connector server configuration are described below. Your deployment might include only a subset of these. Here are two potential scenarios:

- To sync users and groups from Active Directory, the connector must connect to Active Directory.

Port	Source	Target	Description
443	Load Balancer	Connector-va	HTTPS
443	Connector-va	VMware Identity service	HTTPS
443	Browsers	Connector-va	HTTPS
443	Connector-va	vapp-updates.vmware.com	Access to the upgrade server.
8443	Browsers	Connector-va	Administrator Port HTTPS
25		SMTP	TCP port to relay outbound mail
389, 636, 3268, 3269	Connector-va	Active Directory	Default values are shown. These ports are configurable.
445	Connector-va	VMware ThinApp repository	Access to ThinApp repository
5500	Connector-va	RSA SecurID system	Default value is shown. This port is configurable
53	Connector-va	DNS server	TCP/UDP Every virtual appliance must have access to the DNS server on port 53 and allow incoming SSH traffic on port 22
88, 464, 135	Connector-va	Domain controller	TCP/UDP

Active Directory

Active Directory on Windows 2008, 2008 R2, 2012, and 2012 R2 is supported.

Supported Web Browsers to Access the Administration Console

The VMware Identity Manager administration console is a Web-based application you use to manage your tenant. You can access the administration console from the following browsers.

- Internet Explorer 11 for Windows systems

- Google Chrome 42.0 or later for Windows and Mac systems
- Mozilla Firefox 40 or later for Windows and Mac systems
- Safari 6.2.8 and later for Mac systems

Note In Internet Explorer 11, JavaScript must be enabled and cookies allowed to authenticate through VMware Identity Manager.

Supported Browsers to Access the User's My Apps Portal

End users can access the user apps portal from the following browsers.

- Mozilla Firefox (latest)
- Google Chrome (latest)
- Safari (latest)
- Internet Explorer 11
- Microsoft Edge browser
- Native browser and Google Chrome on Android devices
- Safari on iOS devices

Note In Internet Explorer 11, JavaScript must be enabled and cookies allowed to authenticate through VMware Identity Manager.

Deployment Checklists

You can use the deployment checklist to gather the necessary information to install the connector virtual appliance.

Depending on your deployment, you might only need a portion of the network information for your virtual appliances when you create the static IP addresses in the DNS before the installation and during the installation.

Information for Fully Qualified Domain Name

See "Using a Load Balancer to Enable External Access to the Connector," on page 25 for information.

Table 1-1. Fully Qualified Domain Name (FQDN) Information Checklist

Information to Gather	List the Information
connector FQDN	

Network Information for Connector Virtual Appliance

Table 1-2. Network Information Checklist

Information to Gather	List the Information
IP address	
DNS name for this virtual appliance	
Default Gateway address	
Netmask or prefix	

Directory Information

VMware Identity Manager supports integrating with Active Directory or LDAP directory environments.

Table 1-3. Active Directory Domain Controller Information Checklist

Information to Gather	List the Information
Active Directory server name	
Active Directory domain name	
Base DN	
For Active Directory over LDAP, the Bind DN username and password	
For Active Directory with Integrated Windows Authentication, the user name and password of the account that has privileges to join computers to the domain.	

Table 1-4. LDAP Directory Server Information Checklist

Information to Gather	List the Information
LDAP directory server name or IP address	
LDAP directory server port number	
Base DN	
Bind DN username and password	
LDAP search filters for group objects, bind user objects, and user objects	
LDAP attribute names for membership, object UUID, and distinguished name	

SSL Certificates

Table 1-5. SSL Certificate Information Checklist

Information to Gather	List the Information
SSL certificate	
Private key	

Note You can add an SSL certificate after you deploy the connector virtual appliance.

Appliance Administrator Passwords

Create strong passwords for the **admin** user, **root** user, and **sshuser**. Strong passwords should be at least eight characters long and include uppercase and lowercase characters and at least one digit or special character.

Important The **admin** user password must be at least 6 characters in length.

Table 1-6. Administrator Passwords

Information to Gather	List the Information
Appliance administrator account password	
Appliance root account password	
sshuser account password for remote log in	

Deploying VMware Identity Manager Connector 2

To deploy the connector, you install the connector appliance in vSphere, power it on, and activate it using an activation code that you generate in your VMware Identity Manager tenant. You also configure appliance settings such as setting passwords.

After you install and configure the connector, you go to the VMware Identity Manager administration console to set up the connection to your enterprise directory and complete the configuration.

This chapter includes the following topics:

Create Your Identity Provider

Before you can install the connector, your account is created, and you log in to the administration console as the local administrator to retrieve your activation code. This activation code is used to establish communication between your tenant and your connector instance.

Prerequisites

- Request your VMware Identity Manager tenant address. For example, *mycompany.vmwareidentity.com*. VMware uses the vmwareidentity.com domain. When you receive your confirmation, go to your tenant URL and sign in to the VMware Identity Manager administration console using the local admin credentials. This admin is a local user.

Procedure

1. Log in to the administration console with the credentials you received.
2. Click **Accept** to accept the Terms and Conditions agreement.
3. In the administration console, click the **Identity & Access Management** tab.
4. Click **Setup**.
5. On the Connectors page, click **Add Connector**.
6. Enter the connector name.
7. Click **Generate Activation Token.**

   The activation token displays on the page.
8. Copy your connector activation code and save it.

   You use the activation code later when you run the Connector Setup wizard.

You now can install the connector virtual appliance.

Deploy the Connector OVA File

You download the connector OVA file and deploy it using the VMware vSphere Client or vSphere Web Client.

Prerequisites

- Identify the DNS records and host name to use for your connector OVA deployment.
- If using the vSphere Web Client, use either Firefox or Chrome browsers. Do not use Internet Explorer to deploy the OVA file.
- Download the connector OVA file.

Procedure

1 In the vSphere Client or the vSphere Web Client, select **File > Deploy OVF Template**.

2 In the Deploy OVF Template pages, enter the information specific to your deployment of the connector.

Page	Description
Source	Browse to the OVA package location, or enter a specific URL.
OVA Template Details	Verify that you selected the correct version.
License	Read the End User License Agreement and click **Accept**.
Name and Location	Enter a name for the virtual appliance. The name must be unique within the inventory folder and can contain up to 80 characters. Names are case sensitive. Select a location for the virtual appliance.
Host / Cluster	Select the host or cluster to run the deployed template.
Resource Pool	Select the resource pool.
Storage	Select the location to store the virtual machine files.
Disk Format	Select the disk format for the files. For production environments, select a **Thick Provision** format. Use the **Thin Provision** format for evaluation and testing.
Network Mapping	Map the networks in your environment to the networks in the OVF template.
Properties	a In the **Timezone setting** field, select the correct time zone. b The Customer Experience Improvement Program checkbox is selected by default. VMware collects anonymous data about your deployment in order to improve VMware's response to user requirements. Deselect the checkbox if you do not want the data collected. c In the Host Name text box, enter the host name to use. If this is blank, reverse DNS is used to look up the host name. d To configure the static IP address for connector, enter the address for each of the following: Default Gateway, DNS, IP Address, and Netmask. **Important** If any of the four address fields, including Host Name, are left blank, DHCP is used. To configure DHCP, leave the address fields blank.
Ready to Complete	Review your selections and click **Finish**.

Depending on your network speed, the deployment can take several minutes. You can view the progress in the progress dialog box.

3 When the deployment is complete, select the connector appliance, right-click, and select **Power > Power on**.

The connector appliance is initialized. You can go to the **Console** tab to see the details. When the virtual appliance initialization is complete, the console screen displays the connector version and URLs to log in to the connector Setup wizard to complete the setup.

What to do next

Use the Setup wizard to add the activation code and administrative passwords.

Configure Connector Settings

After the connector OVA is deployed and installed, you run the Setup wizard to activate the appliance and configure the administrator passwords.

Prerequisites

- Make sure that the outbound firewall port 443 is open from the connector instance to the vmwareidentity URL. If your network configuration provides Internet access through an HTTP proxy, you must adjust your proxy settings on the appliance to make sure you can establish communication between your connector instance and your tenant. See "Setting Proxy Server Settings for Connector," on page 27.
- You have the activation code. See "Create Your Identity Provider," on page 15.
- Ensure the connector appliance is powered on and you know the connector URL.
- Collect a list of passwords to use for the connector administrator, root account, and sshuser account.

Procedure

1 To run the Setup wizard, enter the connector URL that was displayed in the Console tab after the OVA was deployed.

2 On the Welcome Page, click **Continue**.

3 Create strong passwords for the following connector virtual appliance administrator accounts.

Strong passwords should be at least eight characters long and include uppercase and lowercase characters and at least one digit or special character.

Option	Description
Appliance Administrator	Create the appliance administrator password. The user name is **admin** and cannot be changed. You use this account and password to log into the connector services to manage certificates, appliance passwords and syslog configuration. **Important** The **admin** user password must be at least 6 characters in length.
Root Account	A default VMware root password was used to install the connector appliance. Create a new root password.
sshuser Account	Create the password to use for remote access to the connector appliance.

4 Click **Continue**.

5 On the Activate Connector page, paste the activation code and click **Continue**.

The activation code is verified and the communication between the tenant and your connector instance is established.

The connector setup is complete.

What to do next

Click the link on the Setup is Complete page to go to the tenant administration console. Log in with the temporary administrator user name and password you received for your tenant. Then set up the directory connection and select users and groups to sync to the VMware Identity Manager directory. See Chapter 5, "Integrating with Your Enterprise Directory," on page 31, Chapter 6, "Integrating with Active Directory," on page 33, and Chapter 7, "Integrating with LDAP Directories," on page 47 for more information.

Configure SSL certificates for the connector. See "Using SSL Certificates," on page 20.

Managing Appliance System Configuration Settings

3

After the initial appliance configuration is complete, you can go to the appliance admin pages to install certificates, manage passwords, and monitor system information for the virtual appliance.

The URL to log in to the connector appliance admin pages is https://*connectorFQDN*:8443/cfg. You log in as the admin user with the admin password you created when you configured the connector in the Setup wizard.

Table 3-1. Appliance Configurator Settings

Page Name	Setting Description
Install Certificate	On this page, you install a custom or self-signed certificate for the connector and if the connector is configured with a load balancer, you can install the load balancer's root certificate. The location of the connector root CA certificate is displayed on this page as well. See "Using SSL Certificates," on page 20.
Configure Syslog	On this page, you can enable an external syslog server. Connector appliance logs are sent to this external server. See "Enable the Syslog Server," on page 21.
Change Password	On this page, you can change the connector admin password.
System Security	On this page, you can change the root password for the connector appliance and the password used to log in remotely as an admin.
Log File Locations	A list of the connector log files and their directory locations is displayed on this page. You can bundle the log files into a zip file to download. See "Log File Information," on page 22.

You can also modify the connector URL. See "Modifying the Connector URL," on page 23.

This chapter includes the following topics:

Using SSL Certificates

When the connector appliance is installed, a default SSL server certificate is automatically generated. You can use this self-signed certificate for general testing of your implementation. VMware strongly recommends that you generate and install commercial SSL certificates in your production environment.

A certificate of authority (CA) is a trusted entity that guarantees the identity of the certificate and its creator. When a certificate is signed by a trusted CA, users no longer receive messages asking them to verify the certificate.

If you deploy connector with the self-signed SSL certificate, the root CA certificate must be available as a trusted CA for any client who accesses the connector. The clients can include end user machines, load balancers, proxies, and so on. You can download the root CA from *https://myconnector.domain.com/horizon_workspace_rootca.pem*.

Apply Public Certificate Authority

When the connector is installed, a default SSL server certificate is generated. You should generate and install commercial SSL certificates for your connector environment.

Note If the connector points to a load balancer, the SSL certificate is applied to the load balancer.

Prerequisites

Generate a Certificate Signing Request (CSR) and obtain a valid, signed certificate from a CA. If your organization provides SSL certificates that are signed by a CA, you can use these certificates. The certificate must be in the PEM format.

Procedure

1 Log in to the connector appliance admin pages, https://myconnector.mycompany:8443/cfg, as the admin user.

2 Select **Install Certificate**.

3 In the Terminate SSL on Identity Manager Appliance tab, select **Custom Certificate**.

4 In the **SSL Certificate Chain** text box, paste the host, intermediate, and root certificates, in that order.

The SSL certificate works only if you include the entire certificate chain in the correct order. For each certificate, copy everything between and including the lines -----BEGIN CERTIFICATE----- and -----END CERTIFICATE----

Ensure that the certificate includes the FQDN hostname.

5 Paste the private key in the Private Key text box. Copy everything between ----BEGIN RSA PRIVATE KEY and ---END RSA PRIVATE KEY.

6 Click **Save.**

Example: Certificate Examples

Certificate Chain Example
-----BEGIN CERTIFICATE-----
jlQvt9WdR9Vpg3WQT5+C3HU17bUOwvhp/r0+ ... ... W53+O05j5xsxzDJfWr1lqBlFF/OkIYCPcyK1
-----END CERTIFICATE-----

Certificate Chain Example
-----BEGIN CERTIFICATE-----
WdR9Vpg3WQT5+C3HU17bUOwvhp/rjlQvt90+ ... ... O05j5xsxzDJfWr1lqBlFF/OkIYCPW53+cyK1
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
dR9Vpg3WQTjlQvt9W5+C3HU17bUOwvhp/r0+ ... ... 5j5xsxzDJfWr1lqW53+O0BlFF/OkIYCPcyK1
-----END CERTIFICATE-----

Private Key Example
-----BEGIN RSA PRIVATE KEY-----
jlQvtg3WQT5+C3HU17bU9WdR9VpOwvhp/r0+ ... ... 1lqBlFFW53+O05j5xsxzDJfWr/OkIYCPcyK1
-----END RSA PRIVATE KEY-----

Enable the Syslog Server

Application-level events from the service can be exported to an external syslog server. Operating system events are not exported.

Since most companies do not have unlimited disk space, the virtual appliance does not save the complete logging history. If you want to save more history or create a centralized location for your logging history, you can set up an external syslog server.

If you do not configure a syslog server during the initial configuration, you can configure it later from the Configure Syslog page in the connector appliance admin pages.

Prerequisites

Set up an external syslog server. You can use any of the standard syslog servers available. Several syslog servers include advanced search capabilities.

Procedure

1 Log in to the connector appliance admin pages at https://*myconnector.mycompany*:8443/cfg as the admin user.

2 Select **Configure Syslog** in the left pane.

3 Click **Enable**.

4 Enter the IP address or the FQDN of the syslog server where you want to store the logs.

5 Click **Save.**

A copy of your logs is sent to the syslog server.

Customer Experience Improvement Program

When you install the connector virtual appliance, you can choose to participate in VMware's customer experience improvement program.

If you participate in the program, VMware collects anonymous data about your deployment in order to improve VMware's response to user requirements. No data that identifies your organization is collected.

Before collecting the data, VMware makes anonymous all fields that contain information that is specific to your organization.

Note If your network is configured to access the Internet through HTTP proxy, to send this information, you must adjust your proxy settings on the virtual appliance.

Log File Information

The connector log files can help you debug and troubleshoot. The log files listed below are a common starting point. Additional logs can be found in the `/opt/vmware/horizon/workspace/logs` directory.

Table 3-2. Log Files

Component	Location of Log File	Description
Configurator Logs	`/opt/vmware/horizon/workspace/logs/configurator.log`	Requests that the configurator receives from the REST client and the Web interface.
Connector Logs	`/opt/vmware/horizon/workspace/logs/connector.log`	A record of each request received from the Web interface. Each log entry also includes the request URL, timestamp, and exceptions. No sync actions are recorded.
Apache Tomcat Logs	`/opt/vmware/horizon/workspace/logs/catalina.log`	Apache Tomcat records of messages that are not recorded in other log files.

Collect Log Information

During testing or troubleshooting, the logs can give feedback about the activity and performance of the virtual appliance, as well as information about any problems that occur.

You collect the logs from each appliance that is in your environment.

Procedure

1 Log in to the connector appliance configuration page at https://*myconnector.mycompany*:8443/cfg, as the admin user.

2 Click **Log File Locations** and click **Prepare log bundle**.

The information is collected into a tar.gz file that can be downloaded.

3 Download the prepared bundle.

What to do next

To collect all logs, do this on each appliance.

Manage Your Appliance Passwords

When you configured the virtual appliance, you created passwords for the admin user, root user, and sshuser. You can change these passwords from the Appliance Settings pages.

Make sure that you create strong passwords. Strong passwords should be at least eight characters long and include uppercase and lowercase characters and at least one digit or special character.

Procedure

1 Log in to the connector appliance admin pages, https://myconnector.mycompany:8443/cfg, as the admin user.

2 To change the admin password, select **Change Password**. To change the root or sshuser passwords, select **System Security**.

Important The admin user password must be at least 6 characters in length.

---

3 Enter the new password.

4 Click **Save**.

Modifying the Connector URL

You can change the connector URL by updating the identity provider hostname in the administration console. If you are using the connector as the identity provider, the connector URL is the URL of the login page and is visible to end users.

Procedure

1 Log in to the VMware Identity Manager administration console.

2 Click the **Identity & Access Management** tab, then click the **Identity Providers** tab.

3 In the Identity Providers page, select the identity provider to update.

4 In the **IdP Hostname** field, enter the new hostname.

Use the format ***hostname:port***. Specifying a port is optional. The default port is 443.

For example, **vidm.example.com**.

5 Click **Save**.

Advanced Configuration for the Connector Appliance 4

After you complete the basic connector virtual appliance installation, you might need to complete other configuration tasks such as enabling external access to the connector and configuring redundancy.

This chapter includes the following topics:

Using a Load Balancer to Enable External Access to the Connector

During deployment, the connector virtual appliance is set up inside the internal network. If you want to provide access to the service for users connecting from outside networks, you must install a load balancer, such as Apache, nginx, F5, and so on, in the DMZ.

If you do not use a load balancer, you cannot expand the number of connector virtual appliances. Using multiple connector appliances improves load balancing, failover, and availability to the authentication functionality.

Load Balancer Settings to Configure

Load balancer settings to configure include enabling X-Forwarded-For headers, setting the load balancer timeout correctly, and enabling sticky sessions. In addition, SSL trust must be configured between the connector virtual appliance and the load balancer.

- X-Forwarded-For Headers

  You must enable X-Forwarded-For headers on your load balancer. This determines the authentication method. See the documentation provided by your load balancer vendor for more information.

- Load Balancer Timeout

  For the connector to function correctly, you might need to increase the load balancer request timeout from the default. The value is set in minutes. If the timeout setting is too low, you might see this error, "502 error: The service is currently unavailable."

- Enable Sticky Sessions

  You must enable the sticky session setting on the load balancer if your deployment has multiple connector appliances. The load balancer will then bind a user's session to a specific connector instance.

Apply Connector Root Certificate to the Load Balancer

When the connector virtual appliance is configured with a load balancer, you must establish SSL trust between the load balancer and connector. The connector root certificate must be copied to the load balancer.

The connector certificate can be downloaded from the connector appliance admin pages at https://*myconnector.mycompany*:8443/cfg/ssl.

When the connector domain name points to the load balancer, the SSL certificate can only be applied to the load balancer.

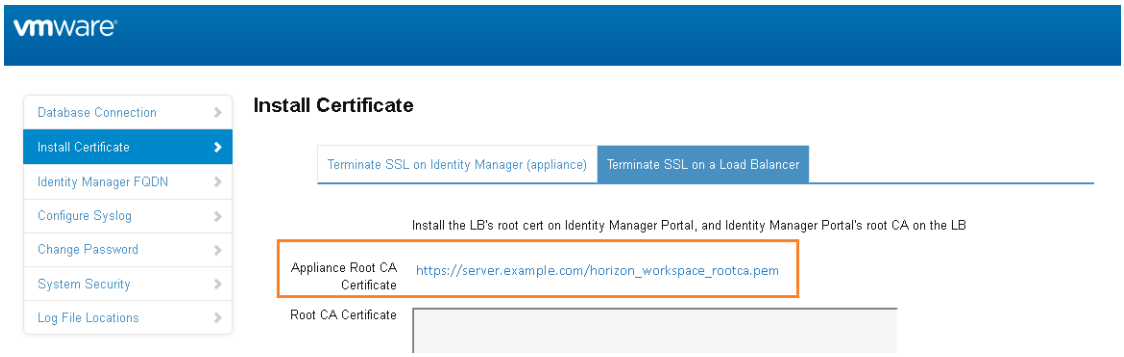
Since the load balancer communicates with the connector virtual appliance, you must copy the connector root CA certificate to the load balancer as a trusted root certificate.

Procedure

1 Log in to the connector appliance admin pages, https://*myconnector.mycompany*:8443/cfg/ssl, as the admin user.

2 Select **Install Certificate**.

3 Select the **Terminate SSL on a Load Balancer** tab and in the **Appliance Root CA Certificate** field, click the link `https://hostname/horizon_workspace_rootca.pem`.



4 Copy everything between and including the lines -----BEGIN CERTIFICATE----- and -----END CERTIFICATE---- and paste the root certificate into the correct location on each of your load balancers. Refer to the documentation provided by your load balancer vendor.

What to do next

Copy and paste the load balancer root certificate to the connector appliance.

Apply Load Balancer Root Certificate to Connector

When the connector virtual appliance is configured with a load balancer, you must establish trust between the load balancer and connector. In addition to copying the connector root certificate to the load balancer, you must copy the load balancer root certificate to connector.

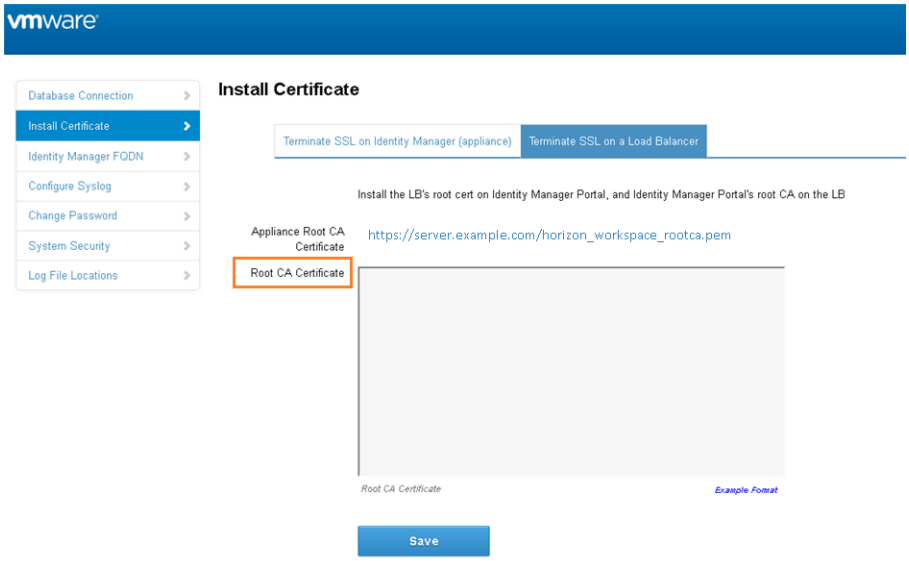
Procedure

1 Obtain the load balancer root certificate.

2 Go to the connector appliance administration page at https://*myconnector.mycompany*:8443/cfg/ssl and log in as the admin user.

3 In the **Install Certificate** page, select the **Terminate SSL on a Load Balancer** tab.

4 Paste the text of the load balancer certificate into the **Root CA Certificate** field.



5 Click **Save**.

Setting Proxy Server Settings for Connector

The connector virtual appliance accesses the VMware Identity Manager cloud services and other Web services on the Internet. If your network configuration provides Internet access through an HTTP proxy, you must adjust your proxy settings on the connector appliance.

Enable your proxy to handle only Internet traffic. To ensure that the proxy is set up correctly, set the parameter for internal traffic to `no-proxy` within the domain.

Note Proxy servers that require authentication are not supported.

Procedure

1 From the vSphere Client, log in as the root user to the connector virtual appliance.

2 Enter `YaST` on the command line to run the `YaST` utility.

3 Select **Network Services** in the left pane, then select **Proxy**.

4 Enter the proxy server URLs in the **HTTP Proxy URL** and **HTTPS Proxy URL** fields.

5 Select **Finish** and exit the `YaST` utility.

6 Restart the Tomcat server on the connector virtual appliance to use the new proxy settings.

```
service horizon-workspace restart
```

Configuring Redundancy

You can set up the connector virtual appliance for failover and redundancy by adding multiple connector virtual appliances in a cluster. If one of the virtual appliances becomes unavailable for any reason, VMware Identity Manager is still available.

Configuring Failover and Redundancy for Connector Appliances

Configure the connector for failover and redundancy by deploying multiple connector virtual appliances in a connector cluster. If one of the appliances shuts down, the connector is still available.

To set up failover, you first install and configure the first connector virtual appliance, create a directory that uses it as the identity provider, and add the connector to the load balancer. You then deploy additional connector appliances and associate them with the Identity Provider page of the first connector, before adding them to the load balancer. As a result, you have multiple connector appliances, all associated with the same directory.

After you set up failover, the connector is highly available. Traffic is distributed to the connector virtual appliances in your cluster based on the load balancer configuration. Specifically, authentication is highly available. If one of the connector instances shuts down, authentication is still available because one of the other connector instances is used. For directory sync, however, in the event of a connector instance failure, you will need to manually select another connector instance as the sync connector. This is because directory sync can only be enabled on one connector at a time.

Prerequisites

You have installed and configured a load balancer. See "Using a Load Balancer to Enable External Access to the Connector," on page 25 for requirements.

Procedure

1 Install the first connector virtual appliance and activate it by obtaining the activation code from the VMware Identity Manager service.

  See Chapter 2, "Deploying VMware Identity Manager Connector," on page 15.

2 Create a directory in the service and select the connector as the identity provider.

3 Add the connector to your load balancer and restart the load balancer.

  - Make sure that the load balancer port is 443. Do not use 8443 as this port number is the administrative port and is unique to each virtual appliance.
  - Apply the connector root certificate to the load balancer and the load balancer root certificate to the connector. See "Using a Load Balancer to Enable External Access to the Connector," on page 25 for information.

4 Change the connector authentication URL to match the load balancer URL.

  a Log in to the VMware Identity Manager administration console.

  b Select the **Identity & Access Management** tab, then select the **Identity Providers** tab.

  c In the Identity Providers page, click the identity provider name for the connector instance.

  d In the **IdP Hostname** field, enter the load balancer fully qualified domain name (FQDN).

    For example, `mylb.mycompany.com`.

  e Click **Save**.

5 Install a new connector virtual appliance.

6 Activate the second connector by obtaining an activation code from the same VMware Identity Manager service instance that you used for the first connector.

7 Add the second connector to the Identity Provider page of the first connector.

   a In the administration console, select the **Identity & Access Management** tab, then select the **Identity Providers** tab.

   b In the Identity Providers page, find the identity provider for the directory that is associated with the first connector and click the identity provider name.

   c In the **Connector** field, select the check box for the second connector.

      Both connectors are now selected for the identity provider.

   d Click **Save**.

      If prompted for a password, specify the Bind DN user password.

8 Add the second connector to your load balancer and restart the load balancer.

9 Repeat steps 5-8 for any additional connector appliances you want to add.

What to do next

- If you had joined an Active Directory domain in the original connector instance, then you need to join the domain in the other connector instances.

   a In the administration console, select the **Identity & Access Management** tab, then click **Setup**.

      The cloned connector instances are listed in the Connectors page.

   b For each connector listed, click **Join Domain** and specify the domain information.

   For more information about Active Directory, see Chapter 6, "Integrating with Active Directory," on page 33.

Enabling Directory Sync on Another Connector Instance in the Event of a Failure

A connector instance handles both directory sync and authentication, or either one of them, based upon your configuration. In the event of a connector instance failure, authentication is handled automatically by another connector instance, as configured in the load balancer. However, for directory sync, you need to modify the directory settings in the VMware Identity Manager service to use another connector instance instead of the original connector instance. Directory sync can only be enabled on one connector at a time.

Procedure

1 Log in to the VMware Identity Manager administration console.

2 Click the **Identity & Access Management** tab, then click **Directories**.

3 Click the directory that was associated with the original connector instance.

   You can view this information in the **Setup > Connectors** page.

4 In the **Directory Sync and Authentication** section of the directory page, in the **Sync Connector** field, select another connector instance.

5 In the **Bind DN Password** field, enter your Active Directory bind account password.

6 Click **Save**.

Adding a Directory After Configuring Failover and Redundancy

If you add a new directory to the VMware Identity Manager service after you have already deployed a cluster for high availability, and you want to make the new directory part of the high availability configuration, you need to add the directory to all the appliances in your cluster.

You do this by adding all the connector instances to the new directory.

Procedure

1 Log in to the VMware Identity Manager administration console.

2 Select the **Identity & Access Management** tab, then select the **Identity Providers** tab.

3 In the Identity Providers page, find the identity provider for the new directory and click the identity provider name.

4 In the **IdP Hostname** field, enter the load balancer FQDN, if it is not already set to the correct load balancer FQDN.

5 In the **Connector(s)** field, select the connector to add.

6 Enter the password and click **Save**.

7 In the Identity Providers page, click the Identity Provider name again and verify that the **IdP Hostname** field displays the correct host name. The **IdP Hostname** field should display the load balancer FQDN. If the name is incorrect, enter the load balancer FQDN and click **Save**.

8 Repeat the preceding steps to add all the connectors listed in the **Connector(s)** field.

Note After you add each connector, check the IdP host name and modify it, if necessary, as described in step 7.

The directory is now associated with all the connectors in your deployment.

Integrating with Your Enterprise Directory

5

You integrate VMware Identity Manager with your enterprise directory to sync users and groups from your enterprise directory to the VMware Identity Manager service.

The following types of directories are supported.

- Active Directory over LDAP
- Active Directory, Integrated Windows Authentication
- LDAP directory

To integrate with your enterprise directory, you perform the following tasks.

- Specify the attributes that you want users to have in the VMware Identity Manager service.
- Create a directory in the VMware Identity Manager service of the same type as your enterprise directory and specify the connection details.
- Map the VMware Identity Manager attributes to attributes used in your Active Directory or LDAP directory.
- Specify the users and groups to sync.
- Sync users and groups.

After you integrate your enterprise directory and perform the initial sync, you can update the configuration, set up a sync schedule to sync regularly, or start a sync at any time.

Important Concepts Related to Directory Integration

Several concepts are integral to understanding how the VMware Identity Manager service integrates with your Active Directory or LDAP directory environment.

Connector

The connector is an on-premise component of the service that you deploy inside your enterprise network. The connector performs the following functions.

- Syncs user and group data from your Active Directory or LDAP directory to the service.
- When being used as an identity provider, authenticates users to the service.

The connector is the default identity provider. You can also use third-party identity providers that support the SAML 2.0 protocol. Use a third-party identity provider for an authentication type the connector does not support, or if the third-party identity provider is preferable based on your enterprise security policy.

Note If you use third-party identity providers, you can either configure the connector to sync user and group data or configure Just-in-Time user provisioning. See the Just-in-Time User Provisioning section in *VMware Identity Manager Administration* for more information.

Directory

The VMware Identity Manager service has its own concept of a directory, corresponding to the Active Directory or LDAP directory in your environment. This directory uses attributes to define users and groups. You create one or more directories in the service and then sync those directories with your Active Directory or LDAP directory. You can create the following directory types in the service.

- Active Directory
  - Active Directory over LDAP. Create this directory type if you plan to connect to a single Active Directory domain environment. For the Active Directory over LDAP directory type, the connector binds to Active Directory using simple bind authentication.
  - Active Directory, Integrated Windows Authentication. Create this directory type if you plan to connect to a multi-domain or multi-forest Active Directory environment. The connector binds to Active Directory using Integrated Windows Authentication.

  The type and number of directories that you create varies depending on your Active Directory environment, such as single domain or multi-domain, and on the type of trust used between domains. In most environments, you create one directory.
- LDAP Directory

The service does not have direct access to your Active Directory or LDAP directory. Only the connector has direct access. Therefore, you associate each directory created in the service with a connector instance.

Worker

When you associate a directory with a connector instance, the connector creates a partition for the associated directory called a worker. A connector instance can have multiple workers associated with it. Each worker acts as an identity provider. You define and configure authentication methods per worker.

The connector syncs user and group data between your Active Directory or LDAP directory and the service through one or more workers.

Important You cannot have two workers of the Active Directory, Integrated Windows Authentication type on the same connector instance.

Integrating with Active Directory 6

You can integrate VMware Identity Manager with your Active Directory deployment to sync users and groups from Active Directory to VMware Identity Manager.

See also "Important Concepts Related to Directory Integration," on page 31.

This chapter includes the following topics:

Active Directory Environments

You can integrate the service with an Active Directory environment that consists of a single Active Directory domain, multiple domains in a single Active Directory forest, or multiple domains across multiple Active Directory forests.

Single Active Directory Domain Environment

A single Active Directory deployment allows you to sync users and groups from a single Active Directory domain.

For this environment, when you add a directory to the service, select the Active Directory over LDAP option.

For more information, see:

- "About Domain Controller Selection (domain_krb.properties file)," on page 35
- "Managing User Attributes that Sync from Active Directory," on page 39
- "Permissions Required for Joining a Domain," on page 40
- "Configuring Active Directory Connection to the Service," on page 41

Multi-Domain, Single Forest Active Directory Environment

A multi-domain, single forest Active Directory deployment allows you to sync users and groups from multiple Active Directory domains within a single forest.

You can configure the service for this Active Directory environment as a single Active Directory, Integrated Windows Authentication directory type or, alternatively, as an Active Directory over LDAP directory type configured with the global catalog option.

- The recommended option is to create a single Active Directory, Integrated Windows Authentication directory type.

  When you add a directory for this environment, select the Active Directory (Integrated Windows Authentication) option.

  For more information, see:

  - "About Domain Controller Selection (domain_krb.properties file)," on page 35
  - "Managing User Attributes that Sync from Active Directory," on page 39
  - "Permissions Required for Joining a Domain," on page 40
  - "Configuring Active Directory Connection to the Service," on page 41
- If Integrated Windows Authentication does not work in your Active Directory environment, create an Active Directory over LDAP directory type and select the global catalog option.

  Some of the limitations with selecting the global catalog option include:

  - The Active Directory object attributes that are replicated to the global catalog are identified in the Active Directory schema as the partial attribute set (PAS). Only these attributes are available for attribute mapping by the service. If necessary, edit the schema to add or remove attributes that are stored in the global catalog.
  - The global catalog stores the group membership (the member attribute) of only universal groups. Only universal groups are synced to the service. If necessary, change the scope of a group from a local domain or global to universal.
  - The bind DN account that you define when configuring a directory in the service must have permissions to read the Token-Groups-Global-And-Universal (TGGAU) attribute.

  Active Directory uses ports 389 and 636 for standard LDAP queries. For global catalog queries, ports 3268 and 3269 are used.

  When you add a directory for the global catalog environment, specify the following during the configuration.

  - Select the Active Directory over LDAP option.
  - Deselect the check box for the option **This Directory supports DNS Service Location**.
  - Select the option **This Directory has a Global Catalog**. When you select this option, the server port number is automatically changed to 3268. Also, because the Base DN is not needed when configuring the global catalog option, the Base DN text box does not display.
  - Add the Active Directory server host name.
  - If your Active Directory requires access over SSL, select the option **This Directory requires all connections to use SSL** and paste the certificate in the text box provided. When you select this option, the server port number is automatically changed to 3269.

Multi-Forest Active Directory Environment with Trust Relationships

A multi-forest Active Directory deployment with trust relationships allows you to sync users and groups from multiple Active Directory domains across forests where two-way trust exists between the domains.

When you add a directory for this environment, select the Active Directory (Integrated Windows Authentication) option.

For more information, see:

- "About Domain Controller Selection (domain_krb.properties file)," on page 35
- "Managing User Attributes that Sync from Active Directory," on page 39
- "Permissions Required for Joining a Domain," on page 40
- "Configuring Active Directory Connection to the Service," on page 41

Multi-Forest Active Directory Environment Without Trust Relationships

A multi-forest Active Directory deployment without trust relationships allows you to sync users and groups from multiple Active Directory domains across forests without a trust relationship between the domains. In this environment, you create multiple directories in the service, one directory for each forest.

The type of directories you create in the service depends on the forest. For forests with multiple domains, select the Active Directory (Integrated Windows Authentication) option. For a forest with a single domain, select the Active Directory over LDAP option.

For more information, see:

- "About Domain Controller Selection (domain_krb.properties file)," on page 35
- "Managing User Attributes that Sync from Active Directory," on page 39
- "Permissions Required for Joining a Domain," on page 40
- "Configuring Active Directory Connection to the Service," on page 41

About Domain Controller Selection (domain_krb.properties file)

The `domain_krb.properties` file determines which domain controllers are used for directories that have DNS Service Location (SRV records) lookup enabled. It contains a list of domain controllers for each domain. The connector creates the file initially, and you must maintain it subsequently. The file overrides DNS Service Location (SRV) lookup.

The following types of directories have DNS Service Location lookup enabled:

- Active Directory over LDAP with the **This Directory supports DNS Service Location** option selected
- Active Directory (Integrated Windows Authentication), which always has DNS Service Location lookup enabled

When you first create a directory that has DNS Service Location lookup enabled, a `domain_krb.properties` file is created automatically in the `/usr/local/horizon/conf` directory of the virtual machine and is auto-populated with domain controllers for each domain. To populate the file, the connector attempts to find domain controllers that are at the same site as the connector and selects two that are reachable and that respond the fastest.

When you create additional directories that have DNS Service Location enabled, or add new domains to an Integrated Windows Authentication directory, the new domains, and a list of domain controllers for them, are added to the file.

You can override the default selection at any time by editing the `domain_krb.properties` file. As a best practice, after you create a directory, view the `domain_krb.properties` file and verify that the domain controllers listed are the optimal ones for your configuration. For a global Active Directory deployment that has multiple domain controllers across different geographical locations, using a domain controller that is in close proximity to the connector ensures faster communication with Active Directory.

You must also update the file manually for any other changes. The following rules apply.

- The `domain_krb.properties` is created in the connector virtual machine. A virtual machine can only have one `domain_krb.properties` file.

- The file is created, and auto-populated with domain controllers for each domain, when you first create a directory that has DNS Service Location lookup enabled.
- Domain controllers for each domain are listed in order of priority. To connect to Active Directory, the connector tries the first domain controller in the list. If it is not reachable, it tries the second one in the list, and so on.
- The file is updated only when you create a new directory that has DNS Service Location lookup enabled or when you add a domain to an Integrated Windows Authentication directory. The new domain and a list of domain controllers for it are added to the file.

  Note that if an entry for a domain already exists in the file, it is not updated. For example, if you created a directory, then deleted it, the original domain entry remains in the file and is not updated.
- The file is not updated automatically in any other scenario. For example, if you delete a directory, the domain entry is not deleted from the file.
- If a domain controller listed in the file is not reachable, edit the file and remove it.
- If you add or edit a domain entry manually, your changes will not be overwritten.

For information on editing the `domain_krb.properties` file, see "Editing the domain_krb.properties file," on page 37.

Important The `/etc/krb5.conf` file must be consistent with the `domain_krb.properties` file. Whenever you update the `domain_krb.properties` file, also update the `krb5.conf` file. See "Editing the domain_krb.properties file," on page 37 and Knowledge Base article 2091744 for more information.

How Domain Controllers are Selected to Auto-Populate the domain_krb.properties File

To auto-populate the `domain_krb.properties` file, domain controllers are selected by first determining the subnet on which the connector resides (based on the IP address and netmask), then using the Active Directory configuration to identify the site of that subnet, getting the list of domain controllers for that site, filtering the list for the appropriate domain, and picking the two domain controllers that respond the fastest.

To detect the domain controllers that are the closest, VMware Identity Manager has the following requirements:

- The subnet of the connector must be present in the Active Directory configuration, or a subnet must be specified in the `runtime-config.properties` file. See "Overriding the Default Subnet Selection," on page 37.

  The subnet is used to determine the site.
- The Active Directory configuration must be site aware.

If the subnet cannot be determined or if your Active Directory configuration is not site aware, DNS Service Location lookup is used to find domain controllers, and the file is populated with a few domain controllers that are reachable. Note that these domain controllers may not be at the same geographical location as the connector, which can result in delays or timeouts while communicating with Active Directory. In this case, edit the `domain_krb.properties` file manually and specify the correct domain controllers to use for each domain. See "Editing the domain_krb.properties file," on page 37.

Sample domain_krb.properties File

```
example.com=host1.example.com:389,host2.example.com:389
```

Overriding the Default Subnet Selection

To auto-populate the `domain_krb.properties` file, the connector attempts to find domain controllers that are at the same site so there is minimal latency between the connector and Active Directory.

To find the site, the connector determines the subnet on which it resides, based on its IP address and netmask, then uses the Active Directory configuration to identify the site for that subnet. If the subnet of the virtual machine is not in Active Directory, or if you want to override the automatic subnet selection, you can specify a subnet in the `runtime-config.properties` file.

Procedure

1 Log in to the connector virtual machine as the root user.

2 Edit the `/usr/local/horizon/conf/runtime-config.properties` file to add the following attribute.

`siteaware.subnet.override=`*`subnet`*

where *subnet* is a subnet for the site whose domain controllers you want to use. For example:

`siteaware.subnet.override=10.100.0.0/20`

3 Save and close the file.

4 Restart the service.

```
service horizon-workspace restart
```

Editing the domain_krb.properties file

The `/usr/local/horizon/conf/domain_krb.properties` file determines the domain controllers to use for directories that have DNS Service Location lookup enabled. You can edit the file at any time to modify the list of domain controllers for a domain, or to add or delete domain entries. Your changes will not be overridden.

The file is initially created and auto-populated by the connector. You need to update it manually in scenarios such as the following:

- If the domain controllers selected by default are not the optimal ones for your configuration, edit the file and specify the domain controllers to use.
- If you delete a directory, delete the corresponding domain entry from the file.
- If any domain controllers in the file are not reachable, remove them from the file.

See also "About Domain Controller Selection (domain_krb.properties file)," on page 35.

Procedure

1 Log in to the connector virtual machine as the root user.

2 Change directories to `/usr/local/horizon/conf`.

3 Edit the `domain_krb.properties` file to add or edit the list of domain to host values.

Use the following format:

`domain=host:port,host2:port,host3:port`

For example:

```
example.com=examplehost1.example.com:389,examplehost2.example.com:389
```

List the domain controllers in order of priority. To connect to Active Directory, the connector tries the first domain controller in the list. If it is not reachable, it tries the second one in the list, and so on.

Important Domain names must be in lowercase.

4 Change the owner of the `domain_krb.properties` file to `horizon` and group to `www` using the following command.

```
chown horizon:www /usr/local/horizon/conf/domain_krb.properties
```

5 Restart the service.

```
service horizon-workspace restart
```

What to do next

After you edit the `domain_krb.properties` file, edit the `/etc/krb5.conf` file. The `krb5.conf` file must be consistent with the `domain_krb.properties` file.

1 Edit the `/etc/krb5.conf` file and update the `realms` section to specify the same domain-to-host values that are used in the `/usr/local/horizon/conf/domain_krb.properties` file. You do not need to specify the port number. For example, if your `domain_krb.properties` file has the domain entry `example.com=examplehost.example.com:389`, you would update the `krb5.conf` file to the following.

```
[realms]
GAUTO-QA.COM = {
auth_to_local = RULE:[1:$0\$1](^GAUTO-QA\.COM\\.*)s/^GAUTO-QA\.COM/GAUTO-QA/
auth_to_local = RULE:[1:$0\$1](^GAUTO-QA\.COM\\.*)s/^GAUTO-QA\.COM/GAUTO-QA/
auth_to_local = RULE:[1:$0\$1](^GAUTO2QA\.GAUTO-QA\.COM\\.*)s/^GAUTO2QA\.GAUTO-
QA\.COM/GAUTO2QA/
auth_to_local = RULE:[1:$0\$1](^GLOBEQE\.NET\\.*)s/^GLOBEQE\.NET/GLOBEQE/
auth_to_local = DEFAULT
kdc = examplehost.example.com
}
```

Note It is possible to have multiple kdc entries. However, it is not a requirement as in most cases there is only a single kdc value. If you choose to define additional kdc values, each line will have a kdc entry which will define a domain controller.

2 Restart the workspace service.

```
service horizon-workspace restart
```

See also Knowledge Base article 2091744.

Troubleshooting domain_krb.properties

Use the following information to troubleshoot the `domain_krb.properties` file.

"Error resolving domain" error

If the `domain_krb.properties` file already includes an entry for a domain, and you try to create a new directory of a different type for the same domain, an "Error resolving domain" occurs. You must edit the `domain_krb.properties` file and manually remove the domain entry before creating the new directory.

Domain controllers are unreachable

Once a domain entry is added to the `domain_krb.properties` file, it is not updated automatically. If any domain controllers listed in the file become unreachable, edit the file manually and remove them.

Managing User Attributes that Sync from Active Directory

During the VMware Identity Manager service directory setup you select Active Directory user attributes and filters to specify which users sync in the VMware Identity Manager directory. You can change the user attributes that sync from the administration console, Identity & Access Management tab, Setup > User Attributes.

Changes that are made and saved in the User Attributes page are added to the Mapped Attributes page in the VMware Identity Manager directory. The attributes changes are updated to the directory with the next sync to Active Directory.

The User Attributes page lists the default directory attributes that can be mapped to Active Directory attributes. You select the attributes that are required, and you can add other Active Directory attributes that you want to sync to the directory. When you add attributes, note that the attribute name you enter is case sensitive. For example, address, Address, and ADDRESS are different attributes.

Table 6-1. Default Active Directory Attributes to Sync to Directory

VMware Identity Manager Directory Attribute Name	Default Mapping to Active Directory Attribute
userPrincipalName	userPrincipalName
distinguishedName	distinguishedName
employeeId	employeeID
domain	canonicalName. Adds the fully qualified domain name of object.
disabled (external user disabled)	userAccountControl. Flagged with UF_Account_Disable When an account is disabled, users cannot log in to access their applications and resources. The resources that users were entitled to are not removed from the account so that when the flag is removed from the account users can log in and access their entitled resources
phone	telephoneNumber
lastName	sn
firstName	givenName
email	mail
userName	sAMAccountName.

Select Attributes to Sync with Directory

When you set up the VMware Identity Manager directory to sync with Active Directory, you specify the user attributes that sync to the directory. Before you set up the directory, you can specify on the User Attributes page which default attributes are required and add additional attributes that you want to map to Active Directory attributes.

When you configure the User Attributes page before the directory is created, you can change default attributes from required to not required, mark attributes as required, and add custom attributes.

After the directory is created, you can change a required attribute to not be required, and you can delete custom attributes. You cannot change an attribute to be a required attribute.

When you add other attributes to sync to the directory, after the directory is created, go to the directory's Mapped Attributes page to map these attributes to Active Directory Attributes.

Important If you plan to sync XenApp resources to VMware Identity Manager, you must make **distinguishedName** a required attribute. You must specify this before creating the VMware Identity Manager directory.

Procedure

1 In the administration console, Identity & Access Management tab, click **Setup > User Attributes**.

2 In the Default Attributes section, review the required attribute list and make appropriate changes to reflect what attributes should be required.

3 In the Attributes section, add the VMware Identity Manager directory attribute name to the list.

4 Click **Save**.

The default attribute status is updated and attributes you added are added on the directory's Mapped Attributes list.

5 After the directory is created, go to the **Manage > Directories** page and select the directory.

6 Click **Sync Settings > Mapped Attributes**.

7 In the drop-down menu for the attributes that you added, select the Active Directory attribute to map to.

8 Click **Save.**

The directory is updated the next time the directory syncs to the Active Directory.

Permissions Required for Joining a Domain

You may need to join the VMware Identity Manager connector to a domain in some cases. For Active Directory over LDAP directories, you can join a domain after creating the directory. For directories of type Active Directory (Integrated Windows Authentication), the connector is joined to the domain automatically when you create the directory. In both scenarios, you are prompted for credentials.

To join a domain, you need Active Directory credentials that have the privilege to "join computer to AD domain". This is configured in Active Directory with the following rights:

- Create Computer Objects
- Delete Computer Objects

When you join a domain, a computer object is created in the default location in Active Directory.

If you do not have the rights to join a domain, or if your company policy requires a custom location for the computer object, follow these steps to join the domain.

1 Ask your Active Directory administrator to create the computer object in Active Directory, in a location determined by your company policy. Provide the host name of the connector. Ensure that you provide the fully-qualified domain name, for example, `server.example.com`.

Tip You can see the host name in the **Host Name** column on the Connectors page in the administration console. Click **Identity & Access Management > Setup > Connectors** to view the Connectors page.

2 After the computer object is created, join the domain using any domain user account in the VMware Identity Manager administration console.

The **Join Domain** command is available on the **Connectors** page, accessed by clicking **Identity & Access Management > Setup > Connectors**.

Configuring Active Directory Connection to the Service

In the administration console, specify the information required to connect to your Active Directory and select users and groups to sync with the VMware Identity Manager directory.

The Active Directory connection options are using Active Directory over LDAP or using Active Directory Integrated Windows Authentication. Active Directory over LDAP connection supports DNS Service Location lookup. With Active Directory Integrated Windows Authentication, you configure the domain to join.

Prerequisites

- Connector installed and the activation code activated.
- Select the required default attributes and add additional attributes on the User Attributes page. See "Select Attributes to Sync with Directory," on page 39.

  Important If you plan to sync XenApp resources with VMware Identity Manager, you must make **distinguishedName** a required attribute. You must make this selection before creating a directory as attributes cannot be changed to be required attributes after a directory is created.

- List of the Active Directory groups and users to sync from Active Directory.
- For Active Directory over LDAP, the information required includes the Base DN, Bind DN, and Bind DN password.

  Note Using a Bind DN user account with a non-expiring password is recommended.

- For Active Directory Integrated Windows Authentication, the information required includes the domain's Bind user UPN address and password.

  Note Using a Bind DN user account with a non-expiring password is recommended.

- If the Active Directory requires access over SSL or STARTTLS, the Root CA certificate of the Active Directory domain controller is required.
- For Active Directory Integrated Windows Authentication, when you have multi-forest Active Directory configured and the Domain Local group contains members from domains in different forests, make sure that the Bind user is added to the Administrators group of the domain in which the Domain Local group resides. If this is not done, these members are missing from the Domain Local group.

Procedure

1 In the administration console, click the **Identity & Access Management** tab.

2 On the Directories page, click **Add Directory**.

3 Enter a name for this VMware Identity Manager directory.

4 Select the type of Active Directory in your environment and configure the connection information.

Option	Description
Active Directory over LDAP	a In the **Sync Connector** field, select the connector to use to sync with Active Directory. b In the **Authentication** field, if this Active Directory is used to authenticate users, click **Yes**. If a third-party identity provider is used to authenticate users, click **No**. After you configure the Active Directory connection to sync users and groups, go to the Identity & Access Management > Manage > Identity Providers page to add the third-party identity provider for authentication. c In the **Directory Search Attribute** field, select the account attribute that contains username. d If the Active Directory uses DNS Service Location lookup, make the following selections. ■ In the **Server Location** section, select the **This Directory supports DNS Service Location** checkbox. A `domain_krb.properties` file, auto-populated with a list of domain controllers, will be created when the directory is created. See "About Domain Controller Selection (domain_krb.properties file)," on page 35 . ■ If the Active Directory requires STARTTLS encryption, select the **This Directory requires all connections to use SSL** check box in the **Certificates** section and copy and paste the Active Directory Root CA certificate into the **SSL Certificate** field. Ensure the certificate is in PEM format and include the "BEGIN CERTIFICATE" and "END CERTIFICATE" lines. **Note** If the Active Directory requires STARTTLS and you do not provide the certificate, you cannot create the directory. e If the Active Directory does not use DNS Service Location lookup, make the following selections. ■ In the **Server Location** section, verify that the **This Directory supports DNS Service Location** checkbox is not selected and enter the Active Directory server host name and port number. To configure the directory as a global catalog, see the Multi-Domain, Single Forest Active Directory Environment section in "Active Directory Environments," on page 33. ■ If the Active Directory requires access over SSL, select the **This Directory requires all connections to use SSL** check box in the **Certificates** section and copy and paste the Active Directory Root CA certificate into the **SSL Certificate** field. Ensure the certificate is in PEM format and include the "BEGIN CERTIFICATE" and "END CERTIFICATE" lines. **Note** If the Active Directory requires SSL and you do not provide the certificate, you cannot create the directory. f In the **Base DN** field, enter the DN from which to start account searches. For example, OU=myUnit,DC=myCorp,DC=com. g In the **Bind DN** field, enter the account that can search for users. For example, CN=binduser,OU=myUnit,DC=myCorp,DC=com. **Note** Using a Bind DN user account with a non-expiring password is recommended. h After you enter the Bind password, click **Test Connection** to verify that the directory can connect to your Active Directory.
Active Directory (Integrated Windows Authentication)	a In the **Sync Connector** field, select the connector to use to sync with Active Directory . b In the **Authentication** field, if this Active Directory is used to authenticate users, click **Yes**.

Option	Description
	If a third-party identity provider is used to authenticate users, click **No**. After you configure the Active Directory connection to sync users and groups, go to the Identity & Access Management > Manage > Identity Providers page to add the third-party identity provider for authentication. c In the **Directory Search Attribute** field, select the account attribute that contains username. d If the Active Directory requires STARTTLS encryption, select the **This Directory requires all connections to use STARTTLS** checkbox in the **Certificates** section and copy and paste the Active Directory Root CA certificate into the **SSL Certificate** field. Ensure the certificate is in PEM format and include the "BEGIN CERTIFICATE" and "END CERTIFICATE" lines. If the directory has multiple domains, add the Root CA certificates for all domains, one at a time. **Note** If the Active Directory requires STARTTLS and you do not provide the certificate, you cannot create the directory. e Enter the name of the Active Directory domain to join. Enter a user name and password that has the rights to join the domain. See "Permissions Required for Joining a Domain," on page 40 for more information. f In the Bind User UPN field, enter the User Principal Name of the user who can authenticate with the domain. For example, username@example.com. **Note** Using a Bind DN user account with a non-expiring password is recommended. g Enter the Bind User password.

5 Click **Save & Next**.

The page with the list of domains appears.

6 For Active Directory over LDAP, the domains are listed with a check mark.

For Active Directory (Integrated Windows Authentication), select the domains that should be associated with this Active Directory connection.

Note If you add a trusting domain after the directory is created, the service does not automatically detect the newly trusting domain. To enable the service to detect the domain, the connector must leave and then rejoin the domain. When the connector rejoins the domain, the trusting domain appears in the list.

Click **Next**.

7 Verify that the VMware Identity Manager directory attribute names are mapped to the correct Active Directory attributes. If not, select the correct Active Directory attribute from the drop-down menu. Click **Next**.

8 Click **+** to select the groups you want to sync from Active Directory to the VMware Identity Manager directory.

The **Sync nested group members** option is enabled by default. When this option is enabled, all the users that belong directly to the group you select as well as all the users that belong to nested groups under it are synced. Note that the nested groups are not synced; only the users that belong to the nested groups are synced. In the VMware Identity Manager directory, these users will be members of the top-level group that you selected for sync.

If this option is disabled, when you specify a group to sync, all the users that belong directly to that group are synced. Users that belong to nested groups under it are not synced. Disabling this option is useful for large Active Directory configurations where traversing a group tree is resource and time intensive. If you disable this option, ensure that you select all the groups whose users you want to sync.

Note When you sync a group, any users that do not have Domain Users as their primary group in Active Directory are not synced.

9 Click **Next**.

10 Click **+** to add additional users. For example, enter as `CN=username,CN=Users,OU=myUnit,DC=myCorp,DC=com`.

To exclude users, create a filter to exclude some types of users. You select the user attribute to filter by, the query rule, and the value.

Click **Next**.

11 Review the page to see how many users and groups are syncing to the directory and to view the sync schedule.

To make changes to users and groups, or to the sync frequency, click the **Edit** links.

12 Click **Sync Directory** to start the sync to the directory.

The connection to Active Directory is established and users and groups are synced from the Active Directory to the VMware Identity Manager directory. The Bind DN user has an administrator role in VMware Identity Manager by default.

What to do next

- If you created a directory that supports DNS Service Location, a `domain_krb.properties` file was created and auto-populated with a list of domain controllers. View the file to verify or edit the list of domain controllers. See "About Domain Controller Selection (domain_krb.properties file)," on page 35.
- Set up authentication methods. After users and groups sync to the directory, if the connector is also used for authentication, you can set up additional authentication methods on the connector. If a third party is the authentication identity provider, configure that identity provider in the connector.

Enabling Users to Reset Expired Active Directory Passwords

You can allow users to change their Active Directory passwords from the VMware Identity Manager login page if the password has expired or if the Active Directory administrator has reset the password, forcing the user to change the password at the next login.

You can enable this option per directory, by selecting the **Allow Change Password** option in the Directory Settings page.

When a user tries to log in with an expired password, the user is prompted to reset the password. The user must enter the old password as well as the new password. The requirements for the new password are determined by the Active Directory password policy. The number of tries allowed also depends on the Active Directory password policy.

Users can reset their Active Directory password from VMware Identity Manager only in the following scenarios:

- If the password has expired.
- If the Active Directory administrator resets the password in Active Directory, forcing the user to change the password at the next login.

The following limitations apply.

- The **Allow Change Password** option is not available for Active Directory environments that use a global catalog.
- The password of a Bind DN user cannot be reset from VMware Identity Manager, even if it expires or the Active Directory administrator resets it.

  Note Using a Bind DN user account with a non-expiring password is recommended.

- Passwords of users whose login names consist of multibyte characters (non-ASCII characters) cannot be reset from VMware Identity Manager.

Prerequisites

- To enable the **Allow Change Password** option, you must use a Bind DN user account and must have write permissions for Active Directory.
- Port 464 must be open on the domain controller.

Procedure

1 In the administration console, click the **Identity & Access Management** tab.

2 In the Directories page, select the directory.

3 In the **Allow Change Password** section, select **Enable change password**.

4 Enter the Bind DN password in the **Bind User Details** section, and click **Save**.

Integrating with LDAP Directories 7

You can integrate your enterprise LDAP directory with VMware Identity Manager to sync users and groups from the LDAP directory to the VMware Identity Manager service.

This chapter includes the following topics:

Limitations of LDAP Directory Integration

The following limitations currently apply to the LDAP directory integration feature.

- You can only integrate a single-domain LDAP directory environment.

  To integrate multiple domains from an LDAP directory, you need to create additional VMware Identity Manager directories, one for each domain.

- The following authentication methods are not supported for VMware Identity Manager directories of type LDAP directory.
  - Kerberos authentication
  - RSA Adaptive Authentication
  - ADFS as a third-party identity provider
  - SecurID
  - Radius authentication with Vasco and SMS Passcode server
- You cannot join an LDAP domain.
- Integration with View or Citrix-published resources is not supported for VMware Identity Manager directories of type LDAP directory.
- User names must not contain spaces. If a user name contains a space, the user is synced but entitlements are not available to the user.
- If you plan to add both Active Directory and LDAP directories, ensure that you do not mark any attributes required in the User Attributes page, except for userName, which can be marked required. The settings in the User Attributes page apply to all directories in the service. If an attribute is marked required, users without that attribute are not synced to the VMware Identity Manager service.
- If you have multiple groups with the same name in your LDAP directory, you must specify unique names for them in the VMware Identity Manager service. You can specify the names when you select the groups to sync.
- The option to allow users to reset expired passwords is not available.

- The `domain_krb.properties` file is not supported.

Integrate an LDAP Directory with the Service

You can integrate your enterprise LDAP directory with VMware Identity Manager to sync users and groups from the LDAP directory to the VMware Identity Manager service.

To integrate your LDAP directory, you create a corresponding VMware Identity Manager directory and sync users and groups from your LDAP directory to the VMware Identity Manager directory. You can set up a regular sync schedule for subsequent updates.

You also select the LDAP attributes that you want to sync for users and map them to VMware Identity Manager attributes.

Your LDAP directory configuration may be based on default schemas or you may have created custom schemas. You may also have defined custom attributes. For VMware Identity Manager to be able to query your LDAP directory to obtain user or group objects, you need to provide the LDAP search filters and attribute names that are applicable to your LDAP directory.

Specifically, you need to provide the following information.

- LDAP search filters for obtaining groups, users, and the bind user
- LDAP attribute names for group membership, UUID, and distinguished name

Certain limitations apply to the LDAP directory integration feature. See "Limitations of LDAP Directory Integration," on page 47.

Prerequisites

- Review the attributes in the **Identity & Access Management > Setup > User Attributes** page and add additional attributes that you want to sync. You map these VMware Identity Manager attributes to your LDAP directory attributes later when you create the directory. These attributes are synced for the users in the directory.

  Note When you make changes to user attributes, consider the effect on other directories in the service. If you plan to add both Active Directory and LDAP directories, ensure that you do not mark any attributes required except for **userName**, which can be marked required. The settings in the User Attributes page apply to all directories in the service. If an attribute is marked required, users without that attribute are not synced to the VMware Identity Manager service.

- A Bind DN user account. Using a Bind DN user account with a non-expiring password is recommended.
- In your LDAP directory, the UUID of users and groups must be in plain text format.
- In your LDAP directory, a domain attribute must exist for all users and groups.

  You map this attribute to the VMware Identity Manager **domain** attribute when you create the VMware Identity Manager directory.
- User names must not contain spaces. If a user name contains a space, the user is synced but entitlements are not available to the user.
- If you use certificate authentication, users must have values for userPrincipalName and email address attributes.

Procedure

1 In the administration console, click the **Identity & Access Management** tab.

2 In the Directories page, click **Add Directory** and select **Add LDAP Directory**.

3 Enter the required information in the Add LDAP Directory page.

Option	Description
Directory Name	A name for the VMware Identity Manager directory.
Directory Sync and Authentication	a In the **Sync Connector** field, select the connector you want to use to sync users and groups from your LDAP directory to the VMware Identity Manager directory. A connector component is always available with the VMware Identity Manager service by default. This connector appears in the drop-down list. If you install multiple VMware Identity Manager appliances for high availability, the connector component of each appears in the list. You do not need a separate connector for an LDAP directory. A connector can support multiple directories, regardless of whether they are Active Directory or LDAP directories. b In the **Authentication** field, if you want to use this LDAP directory to authenticate users, select **Yes**. If you want to use a third-party identity provider to authenticate users, select **No**. After you add the directory connection to sync users and groups, go to the **Identity & Access Management > Manage > Identity Providers page** to add the third-party identity provider for authentication. c In the **Directory Search Attribute** field, specify the LDAP directory attribute to be used for user name. If the attribute is not listed, select **Custom** and type the attribute name. For example, **`cn`**.
Server Location	Enter the LDAP Directory server host and port number. For the server host, you can specify either the fully-qualified domain name or the IP address. For example, **`myLDAPserver.example.com`** or **`100.00.00.0`**. If you have a cluster of servers behind a load balancer, enter the load balancer information instead.
LDAP Configuration	Specify the LDAP search filters and attributes that VMware Identity Manager can use to query your LDAP directory. Default values are provided based on the core LDAP schema. **LDAP Queries** ■ **Get groups**: The search filter for obtaining group objects. For example: **`(objectClass=group)`** ■ **Get bind user**: The search filter for obtaining the bind user object, that is, the user that can bind to the directory. For example: **`(objectClass=person)`** ■ **Get user**: The search filter for obtaining users to sync. For example:**`(&(objectClass=user)(objectCategory=person))`** **Attributes** ■ **Membership**: The attribute that is used in your LDAP directory to define the members of a group. For example: **`member`** ■ **Object UUID**: The attribute that is used in your LDAP directory to define the UUID of a user or group. For example: **`entryUUID`** ■ **Distinguished Name**: The attribute that is used in your LDAP directory for the distinguished name of a user or group. For example: **`entryDN`**

Option	Description
Certificates	If your LDAP directory requires access over SSL, select the **This Directory requires all connections to use SSL** and copy and paste the LDAP directory server's root CA SSL certificate. Ensure the certificate is in PEM format and include the "BEGIN CERTIFICATE" and "END CERTIFICATE" lines.
Bind User Details	**Base DN**: Enter the DN from which to start searches. For example, cn=users,dc=example,dc=com **Bind DN**: Enter the user name to use to bind to the LDAP directory. **Note** Using a Bind DN user account with a non-expiring password is recommended. **Bind DN Password**: Enter the password for the Bind DN user.

4 To test the connection to the LDAP directory server, click **Test Connection**.

If the connection is not successful, check the information you entered and make the appropriate changes.

5 Click **Save & Next**.

6 In the Domains page, verify that the correct domain is listed, then click **Next**.

7 In the Map Attributes page, verify that the VMware Identity Manager attributes are mapped to the correct LDAP attributes.

Important You must specify a mapping for the **domain** attribute.

You can add attributes to the list from the User Attributes page.

8 Click **Next**.

9 In the groups page, click **+** to select the groups you want to sync from the LDAP directory to the VMware Identity Manager directory.

If you have multiple groups with the same name in your LDAP directory, you must specify unique names for them in the groups page.

The **Sync nested group users** option is enabled by default. When this option is enabled, all the users that belong directly to the group you select as well as all the users that belong to nested groups under it are synced. Note that the nested groups are not synced; only the users that belong to the nested groups are synced. In the VMware Identity Manager directory, these users will appear as members of the top-level group that you selected for sync. In effect, the hierarchy under a selected group is flattened and users from all levels appear in VMware Identity Manager as members of the selected group.

If this option is disabled, when you specify a group to sync, all the users that belong directly to that group are synced. Users that belong to nested groups under it are not synced. Disabling this option is useful for large directory configurations where traversing a group tree is resource and time intensive. If you disable this option, ensure that you select all the groups whose users you want to sync.

10 Click **Next**.

11 Click **+** to add additional users. For example, enter **`CN=username,CN=Users,OU=myUnit,DC=myCorp,DC=com`**.

To exclude users, create a filter to exclude some types of users. You select the user attribute to filter by, the query rule, and the value.

Click **Next**.

12 Review the page to see how many users and groups will sync to the directory and to view the default sync schedule.

To make changes to users and groups, or to the sync frequency, click the **Edit** links.

13 Click **Sync Directory** to start the directory sync.

The connection to the LDAP directory is established and users and groups are synced from the LDAP directory to the VMware Identity Manager directory. The Bind DN user has an administrator role in VMware Identity Manager by default.

Deleting a VMware Identity Manager Connector Instance

8

You can delete a VMware Identity Manager Connector instance from the VMware Identity Manager service. A connector instance cannot be deleted if a directory is associated with it.

You may want to delete a connector instance for multiple reasons. For example, you may choose to delete a connector instance when you want to use the same host name for a new connector instance.

Note The ability to delete a connector instance is available in connector version 2.3.1 and later versions.

Procedure

1 Log in to the VMware Identity Manager administration console.

2 Select the **Identity & Access Management** tab, then click **Setup**.

3 If a directory is associated with the connector instance you want to delete, perform the following actions:

   a Click on the directory name in the **Associated Directory** column.

   b Click **Delete Directory**.

4 In the **Setup > Connectors** page, click the **Delete** icon next to the connector instance you want to delete and click **Confirm** in the confirmation dialog box.

   The connector instance is deleted from the VMware Identity Manager service.

5 (Optional) Delete the connector virtual appliance.

   a Log in to the vSphere Client or vSphere Web Client.

   b Navigate to the connector virtual appliance.

   c Right-click and select **Power > Power Off**.

   d Right-click and select **Delete from Disk**.

Index