VMware Identity Manager Cloud Deployment

JULY 2018

VMware Identity Manager

vmware®

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

https://docs.vmware.com/

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 Cloud Deployment

VMware Identity Manager Cloud Deployment provides information about the deployment scenarios available for using the VMware Identity Manager™ cloud service. It also provides information about installing and configuring the VMware Identity Manager Connector virtual appliance in outbound-only connection mode. Additionally, it explains how to integrate your enterprise directory and sync users and groups to the VMware Identity Manager service.

For information about installing and configuring the VMware Identity Manager Connector virtual appliance in legacy mode, see *Installing and Configuring VMware Identity Manager Connector (Legacy Mode)*.

For information about using VMware Identity Manager with VMware AirWatch®, see the relevant sections of this document, *Guide to Deploying Workspace ONE*, and the AirWatch documentation.

Intended Audience

The information is written for experienced Windows and Linux system administrators who are familiar with VMware technologies, particularly vCenter™, ESX™, and vSphere®, and with networking concepts, Active Directory, and databases.

Knowledge of other technologies, such as RSA Adaptive Authentication, RSA SecurID, and RADIUS is also helpful if you plan to implement those features.

VMware Technical Publications Glossary

VMware Technical Publications provides a glossary of terms that might be unfamiliar to you. For definitions of terms as they are used in VMware technical documentation, go to http://www.vmware.com/support/pubs.

1 Deployment Models

To use your VMware Identity Manager tenant, you need an on-premises component for user authentication and directory integration. Two main types of deployment models are available, one that integrates with a VMware AirWatch® deployment, and one that does not require AirWatch and uses the VMware Identity Manager connector.

You can also combine deployment models if you require functionality that is not supported in one of the models.

- Deployment Model using AirWatch Cloud Connector

  If you have an existing AirWatch deployment, you can integrate your VMware Identity Manager tenant with it quickly. In this model, user and group sync from your enterprise directory and user authentication are handled by AirWatch. There are no additional deployment requirements for VMware Identity Manager.

  Note that integrating VMware Identity Manager with resources such as Horizon 7 and Citrix-published resources is not supported in this model. Only integration with Web applications and native mobile applications is supported.

  See Deployment Model Using AirWatch Cloud Connector.

- Deployment Model using VMware Identity Manager Connector (in outbound-only connection mode)

  To use your VMware Identity Manager tenant in a scenario that does not require an AirWatch deployment, you install the VMware Identity Manager connector virtual appliance on premises. The connector connects the tenant with on-premises services such as Active Directory. In this model, user and group sync from your enterprise directory and user authentication are handled by the VMware Identity Manager connector. The connector is installed in outbound-only connection mode and does not require inbound firewall port 443 to be opened.

  See Deployment Model Using VMware Identity Manager Connector in Outbound-Only Connection Mode.

  - Adding Kerberos authentication support to your deployment

    You can add Kerberos authentication for internal users (which requires inbound connection mode) to your deployment based on outbound-only connection mode connectors.

    See Adding Kerberos Authentication Support to Your Deployment.

- VMware Identity Manager Connector Legacy Deployment Model

The VMware Identity Manager connector can also be installed in legacy mode, which requires opening inbound firewall port 443 to the connector.

For information about installing and configuring the connector in this model, see *Installing and Configuring VMware Identity Manager Connector (Legacy Mode)*.

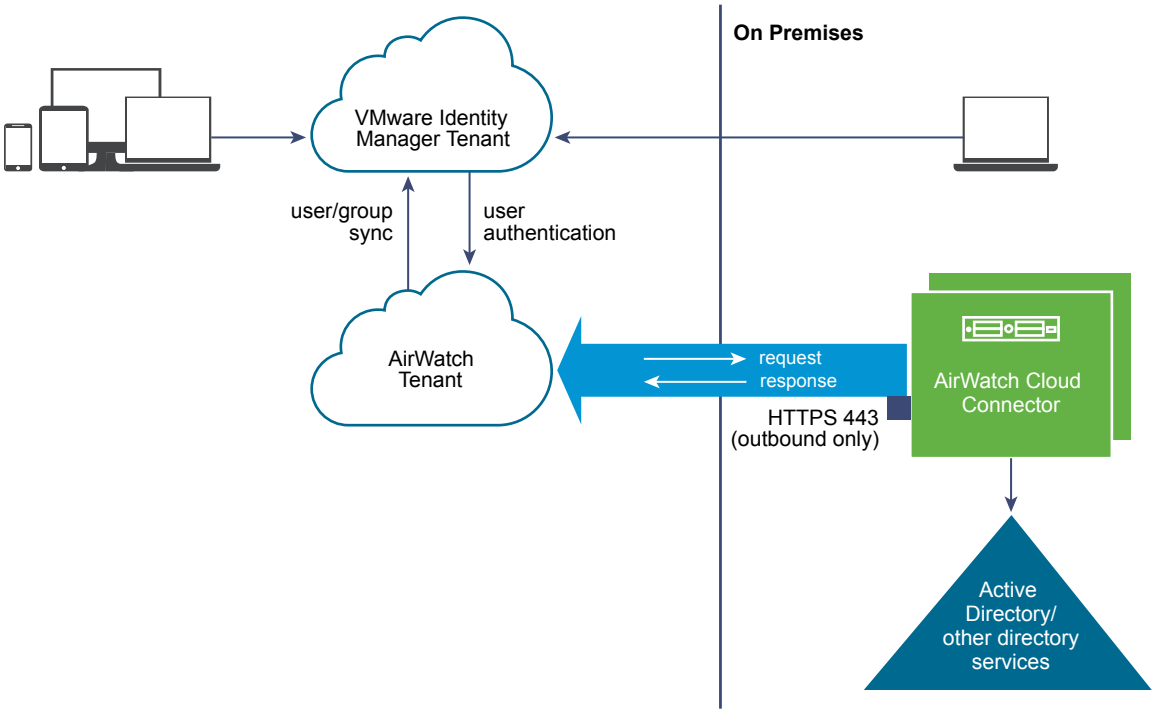
This chapter includes the following topics:

Deployment Model Using AirWatch Cloud Connector

If you have an existing AirWatch deployment, you can integrate your VMware Identity Manager tenant with it. In this model, user and group sync from your enterprise directory and user authentication are handled by AirWatch. There are no additional deployment requirements for VMware Identity Manager.

Note that integrating VMware Identity Manager with resources such as Horizon 7 or Citrix-published resources is not supported in this model. Only integration with Web applications and native mobile applications is supported.

Figure 1-1. Using AirWatch Cloud Connector



Prerequisites

You must have the following components.

- A VMware Identity Manager tenant
- An AirWatch tenant

- An AirWatch Cloud Connector instance deployed on premises and integrated with your enterprise directory

Port Requirements

There are no additional port requirements for VMware Identity Manager. The VMware Identity Manager tenant only communicates with the AirWatch tenant.

For AirWatch deployment requirements, see the AirWatch documentation.

Supported Authentication Methods

This deployment model supports the following authentication methods. These methods are available through the VMware Identity Manager Built-in identity provider.

- Password (AirWatch Connector)
- Mobile SSO (for iOS)
- Mobile SSO (for Android)
- Device Compliance (with AirWatch)
- Certificate (cloud deployment)
- VMware Verify

In addition, inbound SAML through a third-party identity provider is also available.

Supported Directory Integrations

You integrate your enterprise directory with AirWatch. See the AirWatch documentation for the types of directories supported.

Supported Resources

You can integrate the following types of resources with VMware Identity Manager in this deployment model.

- Web applications
- Native mobile applications

You cannot integrate the following resources with VMware Identity Manager in this deployment model.

- VMware Horizon® 7, Horizon 6, or View desktop and application pools
- Citrix-published resources
- VMware Horizon® Cloud Service™ applications and desktops
- VMware ThinApp packaged applications

Additional Information

For additional information, see the following documentation.

- *Guide to Deploying VMware Workspace ONE*
- AirWatch documentation

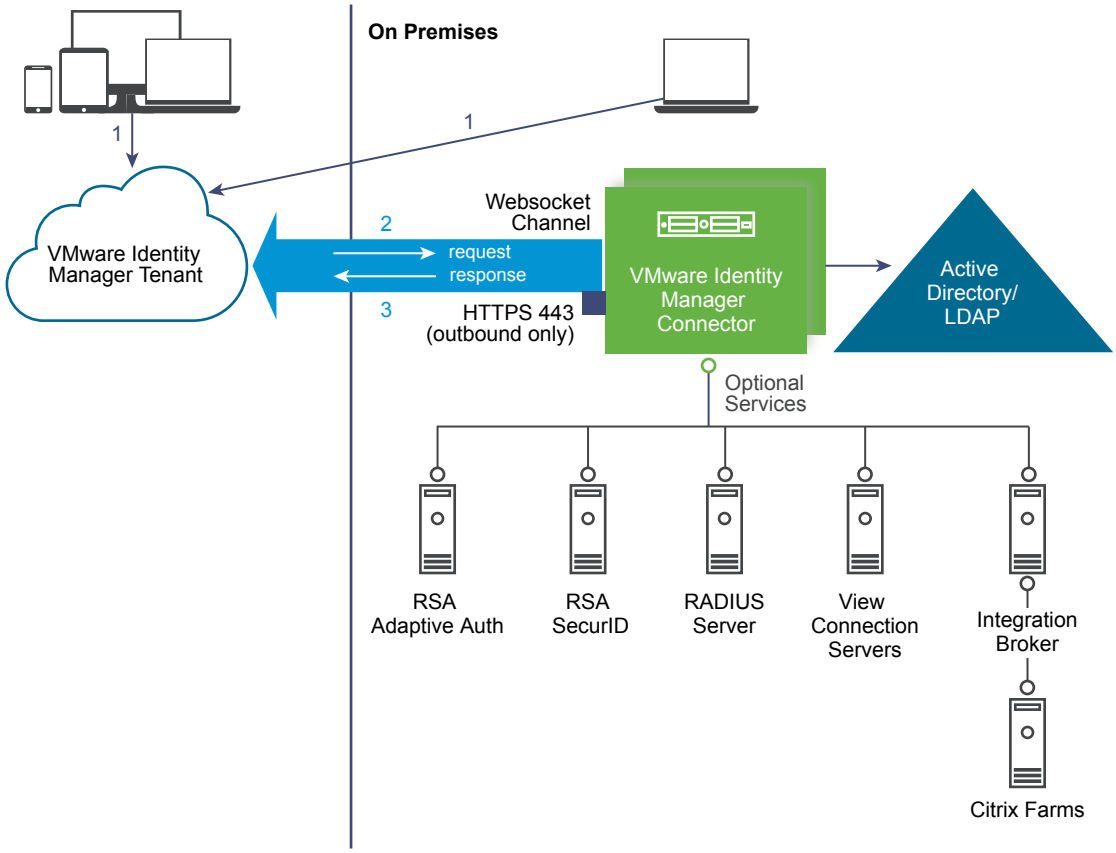
Important The rest of this document does not pertain to the AirWatch deployment model. It only pertains to deployment models that use the VMware Identity Manager connector in outbound-only connection mode.

Deployment Model Using VMware Identity Manager Connector in Outbound-Only Connection Mode

To use your VMware Identity Manager tenant without an AirWatch deployment, you install the VMware Identity Manager connector virtual appliance on premises in outbound-only connection mode. In this model, user and group sync from your enterprise directory and user authentication are handled by the VMware Identity Manager connector. Note that some authentication methods do not require the connector and are managed directly by the service.

The connector can also sync resources, such as Horizon 7 desktops and applications, to the VMware Identity Manager service.

Figure 1-2. Using VMware Identity Manager Connector



Port Requirements

The connector is installed in outbound-only connection mode and does not require inbound port 443 to be opened. The connector communicates with the VMware Identity Manager service through a Websocket-based communication channel.

For the list of ports used, see System and Network Configuration Requirements.

Supported Authentication Methods

This deployment model supports all authentication methods. Some of these authentication methods do not require the connector and are managed directly by the service through the Built-in identity provider.

- Password - uses the connector
- RSA Adaptive Authentication - uses the connector
- RSA SecurID - uses the connector
- RADIUS - uses the connector
- Certificate (cloud deployment) - through the Built-in identity provider
- VMware Verify - through the Built-in identity provider
- Mobile SSO (iOS) - through the Built-in identity provider

- Mobile SSO (Android) - through the Built-in identity provider
- Inbound SAML through a third-party identity provider

Note For information on using Kerberos, see Adding Kerberos Authentication Support to Your Deployment.

Supported Directory Integrations

You can integrate the following types of enterprise directories with VMware Identity Manager.

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

  If you plan to integrate an LDAP directory, see Limitations of LDAP Directory Integration first.

Alternatively, you can use Just-in-Time provisioning to create users in the VMware Identity Manager service dynamically at login, using SAML assertions sent by a third-party identity provider.

Supported Resources

You can integrate the following types of resources with VMware Identity Manager.

- Web applications
- VMware Horizon 7, Horizon 6, or View desktop and application pools
- Citrix-published resources
- VMware Horizon Cloud Service applications and desktops
- ThinApp packaged applications

Additional Information

- The rest of this document contains information about installing and configuring the VMware Identity Manager connector. The information applies only to the deployment model that uses the VMware Identity Manager Connector in outbound-only connection mode.
- See also "Configuring User Authentication in VMware Identity Manager" in the *VMware Identity Manager Administration Guide*.

Adding Kerberos Authentication Support to Your Deployment

You can add Kerberos authentication for internal users, which requires inbound connection mode, to your deployment based on VMware Identity Manager outbound-only connection mode connectors. The same connectors can be configured to use Kerberos authentication for users coming from the internal network and another authentication method for users coming from outside. This can be achieved by defining authentication policies based on network ranges.

Note The process to configure high availability of Kerberos authentication is different.

For more information, see Chapter 5 Adding Kerberos Authentication Support to Your VMware Identity Manager Connector Deployment.

Preparing to Install VMware Identity Manager Connector

2

VMware Identity Manager Connector is a virtual appliance that you deploy in your vSphere environment on premises. Before you deploy the connector, review the requirements and perform the required tasks.

This chapter includes the following topics:

System and Network Configuration Requirements

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

Supported vSphere and ESX Versions

You install the virtual appliance in vCenter Server. The following versions of vSphere and ESX server are supported:

- 5.5 and later
- 6.0 and later

The VMware vSphere® Web Client is required to deploy the OVA file and access the deployed virtual appliance remotely.

VMware Identity Manager Connector Virtual Appliance Requirements

Ensure that you meet the requirements for the number of servers and the resources allocated to each server.

Number of Users	Up to 1,000	1,000-10,000	10,000-25,000	25,000-50,000	50,000-100,1000
Number of connector servers	1 server	2 load-balanced servers	2 load-balanced servers	2 load-balanced servers	2 load-balanced servers
CPU (per server)	2 CPU	4 CPU	4 CPU	4 CPU	4 CPU

Number of Users	Up to 1,000	1,000-10,000	10,000-25,000	25,000-50,000	50,000-100,1000
RAM (per server)	6 GB	6 GB	8 GB	16 GB	16 GB
Disk space (per server)	60 GB	60 GB	60 GB	60 GB	60 GB

Network Configuration Requirements

Component	Minimum Requirement
DNS record and static IP address	See Create DNS Records and IP Addresses.
Firewall port	Ensure that the outbound firewall port 443 is open from the connector instance to your VMware Identity Manager URL.

Port Requirements

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

Port	Source	Target	Description
443	Connector virtual appliance	VMware Identity Manager service	HTTPS
443, 80	Connector virtual appliance	vapp-updates.vmware.com	Access to the upgrade server
8443	Browsers	Connector virtual appliance	HTTPS Administrator Port
443	Browsers	Connector virtual appliance	HTTPS This port is only required for a connector being used in inbound mode. If Kerberos authentication is configured on the connector, this port is required.
389, 636, 3268, 3269	Connector virtual appliance	Active Directory	Default values are shown. These ports are configurable.
5500	Connector virtual appliance	RSA SecurID system	Default value is shown. This port is configurable
53	Connector virtual appliance	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, 445	Connector virtual appliance	Domain controller	TCP/UDP
389, 443	Connector virtual appliance	View Connection Server	Access to View Connection Server instances for Horizon/View integrations

Port	Source	Target	Description
445	Connector virtual appliance	VMware ThinApp repository	Access to ThinApp repository
80, 443	Connector virtual appliance	Integration Broker server	TCP Connection to the Integration Broker server. Port option depends on whether a certificate is installed on the Integration Broker server.
514	Connector virtual appliance	syslog server	UDP For external syslog server, if configured

Supported Directories

You integrate your enterprise directory with VMware Identity Manager and sync users and groups from your enterprise directory to the service. You can integrate the following types of directories.

- 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.

  VMware Identity Manager supports Active Directory on Windows 2008, 2008 R2, 2012, and 2012 R2, with a Domain functional level and Forest functional level of Windows 2003 and later.

  Note A higher functional level may be required for some features. For example, to allow users to change Active Directory passwords from Workspace ONE, the Domain functional level must be Windows 2008 or later.

- An LDAP directory

Your directory must be accessible to the connector virtual appliance.

Note You can also create local directories in the VMware Identity Manager service.

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 latest versions of Mozilla Firefox, Google Chrome, Safari, Microsoft Edge, and Internet Explorer 11.

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

Supported Browsers to Access the Workspace ONE Portal

End users can access the Workspace ONE 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.

Create DNS Records and IP Addresses

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

Configuring reverse lookup is optional. When you implement reverse lookup, you must define a PTR record on the DNS server so the virtual appliance uses the correct network configuration.

You can use the following sample list of DNS records when you talk to your network administrator. Replace the sample information with information from your environment. This example shows forward DNS records and IP addresses.

Table 2-1. Examples of Forward DNS Records and IP Addresses

Domain Name	Resource Type	IP Address
myidentitymanager.company.com	A	10.28.128.3

This example shows reverse DNS records and IP addresses.

Table 2-2. Examples of Reverse DNS Records and IP Addresses

IP Address	Resource Type	Host Name
10.28.128.3	PTR	myidentitymanager.company.com

After you complete the DNS configuration, verify that the reverse DNS lookup is properly configured. For example, the virtual appliance command `host IPaddress` must resolve to the DNS name lookup.

Planning for Kerberos Authentication

If you plan to set up Kerberos authentication, note that the connector host name must match the Active Directory domain to which the connector is joined. For example, if the Active Directory domain is sales.example.com, the connector host name must be *connectorhost*.sales.example.com.

If you cannot assign a hostname that matches the Active Directory domain structure, you need to configure the connector and Active Directory manually. See the Knowledge Base for information.

Using a Unix/Linux-based DNS Server

If you are using a Unix or Linux-based DNS server and plan to join connector to the Active Directory domain, make sure that the appropriate service (SRV) resource records are created for each Active Directory domain controller.

Note If you have a load balancer with a Virtual IP address (VIP) in front of the DNS servers, note that VMware Identity Manager does not support using a VIP. You can specify multiple DNS servers separated by a comma.

Deployment Checklists

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

Information for Fully Qualified Domain Name

Table 2-3. Fully Qualified Domain Name (FQDN) Information Checklist

Information to Gather	List the Information
connector FQDN	**Note** If you plan to set up Kerberos authentication, the connector host name must match the Active Directory domain to which the connector is joined. For example, if the Active Directory domain is sales.example.com, the connector host name must be *connectorhost*.sales.example.com. If you cannot assign a hostname that matches the Active Directory domain structure, you need to configure the connector and Active Directory manually. See the Knowledge Base for information.

Network Information for Connector Virtual Appliance

Table 2-4. Network Information Checklist

Information to Gather	List the Information
IP address	**Note** You must use a static IP address and it must have a PTR and an A record defined in the DNS.
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 2-5. 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 2-6. 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

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

Table 2-7. SSL Certificate Information Checklist

Information to Gather	List the Information
SSL certificate	
Private key	

Deploying the VMware Identity Manager Connector

3

To deploy the VMware Identity Manager connector, you install the connector virtual appliance in vCenter Server, power it on, and activate it using an activation code that you generate in the VMware Identity Manager administration console. 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, enable authentication adapters on the connector, and enable outbound mode for the connector.

1 Generate Activation Code for Connector

2 Install and Configure the Connector Virtual Appliance

   To deploy the connector, you install the connector virtual appliance in vCenter Server using the vSphere Web Client, power it on, and activate it using the activation code that you generated in the VMware Identity Manager administration console.

3 Set up a Directory

   After you deploy the connector virtual appliance, set up a directory in the VMware Identity Manager administration console. You can sync users and groups from your enterprise directory to the VMware Identity Manager service.

4 Enable Authentication Adapters on the VMware Identity Manager Connector

   Several authentication adapters are available for the VMware Identity Manager Connector in outbound mode, including PasswordIdpAdapter, RSAAIdpAdapter, SecurIDAdapter, and RadiusAuthAdapter. Configure and enable the adapters that you intend to use.

5 Enable Outbound Mode for the VMware Identity Manager Connector

   To enable outbound-only connection mode for the VMware Identity Manager Connector, associate the connector with the Built-in identity provider.

Generate Activation Code for Connector

Before you install the VMware Identity Manager connector, log in to your VMware Identity Manager tenant administration console as the local administrator and generate an activation code for the connector. This activation code is used to establish communication between your tenant and your connector instance.

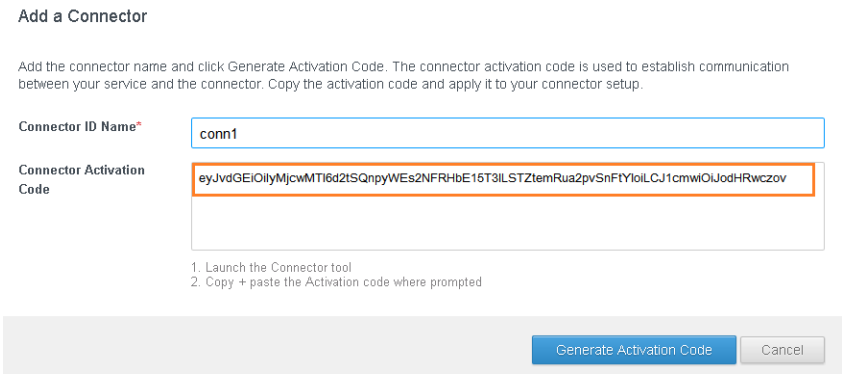
Prerequisites

You have 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 you received. This admin is a local user.

Procedure

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

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



   You need the activation code later when you deploy the connector.

You can now install the connector virtual appliance.

Install and Configure the Connector Virtual Appliance

To deploy the connector, you install the connector virtual appliance in vCenter Server using the vSphere Web Client, power it on, and activate it using the activation code that you generated in the VMware Identity Manager administration console.

Prerequisites

- Download the connector OVA file from the VMware Identity Manager product page on my.vmware.com.

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

  Note If you plan to set up Kerberos authentication, the connector host name must match the Active Directory domain to which the connector is joined. For example, if the Active Directory domain is sales.example.com, the connector host name must be *connectorhost*.sales.example.com.

  If you cannot assign a hostname that matches the Active Directory domain structure, you need to configure the connector and Active Directory manually. See the Knowledge Base for information.

Procedure

1. In the vSphere Web Client, right-click any inventory object in which a virtual machine can be deployed, such as a host, cluster, or folder, and select **Deploy OVF Template**.
2. Follow the Deploy OVF Template wizard to deploy the VMware Identity Manager connector template.
   a. In the Select template page, select **Local file**, click **Browse** to select the connector OVA file you downloaded, and click **Next**.
   b. In the Select name and location page, enter a unique name for the connector virtual appliance, select a datacenter or folder as the deployment location, and click **Next**.
   c. In the Select a resource page, select the host, cluster, resource pool, or vApp where you want to run the connector virtual appliance, and click **Next**.
   d. In the Review details page, review the connector template details and click **Next**.
   e. In the Accept license agreements page, read and accept the license agreement, then click **Next**.
   f. In the Select storage page, select the datastore or datastore cluster in which to store the virtual appliance files, then click **Next**.

      Also select the virtual disk format for the files. For production environments, select a **Thick Provision** format. Use the **Thin Provision** format for evaluation and testing.
   g. In the Select networks page, select the destination network to which you want to connect the connector virtual appliance, then click **Next**.

h In the Customize template page, set the application and network properties.

Option	Description
Application Properties	**Join the VMware Customer Experience Improvement Program** This product participates in VMware's Customer Experience Improvement Program ("CEIP"). Details regarding the data collected through CEIP and the purposes for which it is used by VMware are set forth at the Trust & Assurance Center at http://www.vmware.com/trustvmware/ceip.html. If you prefer not to participate in VMware's CEIP for this product, uncheck the box. You can also join or leave the CEIP for this product at any time after installation. **Note** If your network is configured to access the Internet through HTTP proxy, to send the data collected through CEIP to VMware, you must adjust the proxy settings on the connector virtual appliance. You can change the proxy settings after deploying the connector. **Note** The CEIP is only applicable for on-premises installations of VMware Identity Manager. Make your selections when you install the VMware Identity Manager service. You can also join or leave the CEIP at any time from the administration console after installation. **Timezone Setting** Select the correct timezone.
Networking Properties	Enter values for **DNS**, **Default Gateway**, **IP Address**, and **Netmask** to configure the static IP address for the connector. If any of these four address fields, or the **Host Name** field, are left blank, DHCP is used. In the **Host Name (FQDN)** text box, enter the fully-qualified host name to use for the connector virtual appliance. If this is blank, reverse DNS is used to look up the host name.

i In the Ready to complete page, review your selections, make any adjustments if needed, and click **Finish**.

Depending on your network speed, the deployment can take several minutes.

3 When the deployment is complete and the connector virtual appliance appears under the inventory object in which you deployed it, right-click the connector virtual appliance and select **Power > Power on**.

The connector virtual appliance is initialized. You can go to the **Summary** tab and click the console to see the details. When the virtual appliance initialization is complete, the console displays the connector version and the URL for the Setup wizard.

4 To run the Setup wizard, point your browser to the connector URL displayed in the console, https://*connectorFQDN*.

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

6 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 in to 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.

7 Click **Continue**.

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

The activation code is verified and the communication between the VMware Identity Manager service 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 administration console. Log in with the temporary administrator user name and password you received for your tenant. Then set up the directory connection.

Set up a Directory

After you deploy the connector virtual appliance, set up a directory in the VMware Identity Manager administration console. You can sync users and groups from your enterprise directory to the VMware Identity Manager service.

VMware Identity Manager supports integrating the following types of directories.

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

See Chapter 6 Integrating Your Enterprise Directory with VMware Identity Manager for more information.

Note You can also create local directories in the VMware Identity Manager service. See Chapter 7 Using Local Directories.

Procedure

1 Click the link on the Setup is Complete page, which is displayed after you activate the connector.

The **Identity & Access Management > Directories** tab is displayed.

2 Click **Add Directory** and select the type of directory you want to add.

3 Follow the wizard to enter the directory configuration information, select groups and users to sync, and sync users to the VMware Identity Manager service.

See Chapter 6 Integrating Your Enterprise Directory with VMware Identity Manager for information on how to set up a directory.

What to do next

Click the **Users & Groups** tab and verify that users have been synced.

Enable Authentication Adapters on the VMware Identity Manager Connector

Several authentication adapters are available for the VMware Identity Manager Connector in outbound mode, including PasswordIdpAdapter, RSAAIdpAdapter, SecurIDAdapter, and RadiusAuthAdapter. Configure and enable the adapters that you intend to use.

When you created the directory, the Password authentication method was automatically enabled for it. The PasswordIdpAdapter was configured with the information you provided for the directory.

Procedure

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

2 Click **Setup**, then click the **Connectors** tab.

The connector you deployed is listed.

3 Click the link in the **Worker** column.

4 Click the **Auth Adapters** tab.

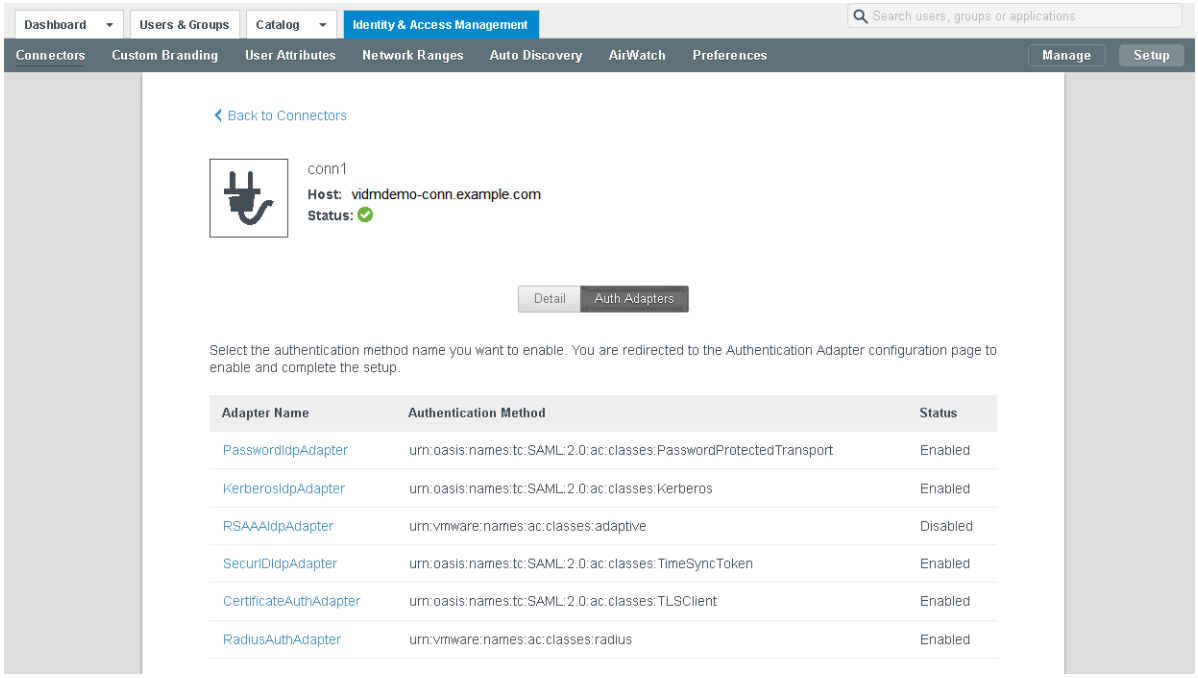
All available authentication adapters for the connector are listed.

If you have already set up a directory, the PasswordIdpAdapter is already configured and enabled, with the configuration information you specified while creating the directory.

5 Configure and enable the authentication adapters you want to use by clicking on the link for each and entering the configuration information. You must enable at least one authentication adapter.

For information on configuring specific authentication adapters, see the *VMware Identity Manager Administration Guide*.

For example:



Enable Outbound Mode for the VMware Identity Manager Connector

To enable outbound-only connection mode for the VMware Identity Manager Connector, associate the connector with the Built-in identity provider.

The Built-in identity provider is available by default in the VMware Identity Manager service and provides additional built-in authentication methods such as VMware Verify. For information about the Built-in identity provider, see the *VMware Identity Manager Administration Guide*.

Note The connector can be used in both outbound and regular mode simultaneously. Even if you enable outbound mode, you can still configure Kerberos authentication for internal users using authentication methods and policies.

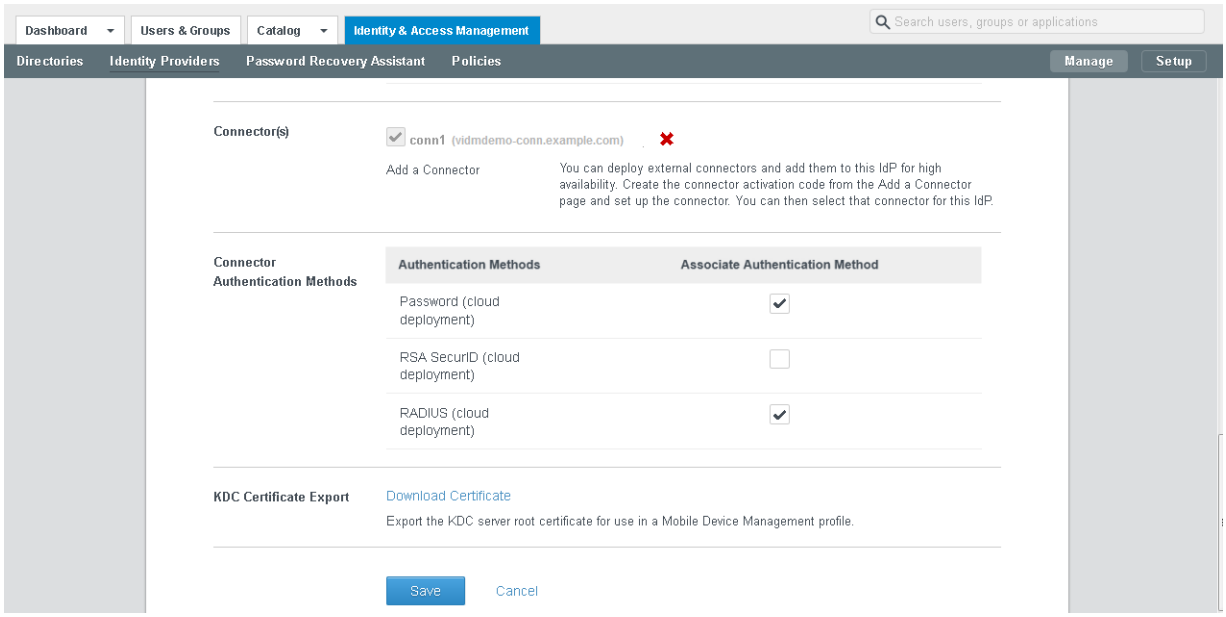
Procedure

1. In the administration console **Identity & Access Management** tab, click **Manage**.
2. Click the **Identity Providers** tab.
3. Click the **Built-in** link.
4. Enter the following information.

Option	Description
Users	Select the directory or domains that will use the Built-in identity provider.
Network	Select the network ranges that will use the Built-in identity provider.

Option	Description
Connector(s)	Select the connector that you set up. **Note** Later, when you add additional connectors for high availability, select and add all of them here to associate them with the Built-in identity provider. VMware Identity Manager automatically distributes traffic among all the connectors associated with the Built-in identity provider. A load balancer is not required.
Connector Authentication Methods	The deployment methods that you enabled for the connector are listed. Select the authentication methods that you want to use. The PasswordIdpAdapter, which was automatically configured and enabled when you created a directory, is displayed on this page as **Password (cloud deployed)**, which denotes that it is used with the connector in outbound mode.

For example:



5 Click **Save** to save the Built-in identity provider configuration.

6 Edit policies to use the authentication methods that you enabled.

   a In the **Identity & Access Management** tab, click **Manage**.

   b Click the **Policies** tab and click the policy you want to edit.

   c Under **Policy Rules**, for the rule you want to edit, click the link in the **Authentication Method** column.

   d In the Edit Policy Rule page, select the authentication method that you want to use for this rule.

   e Click **OK**.

   f Click **Save**.

   For more information about configuring policies, see the *VMware Identity Manager Administration Guide*.

The outbound mode of the connector is now enabled. When a user logs in using one of the authentication methods that you enabled for the connector in the Built-in identity provider page, an HTTP redirect to the connector is not required.

Configuring High Availability for the VMware Identity Manager Connector

4

You can set up the VMware Identity Manager Connector for high availability and failover by adding multiple connector instances in a cluster. If one of the connector instances becomes unavailable for any reason, other instances will still be available.

To create a cluster, you install new connector instances and configure them in exactly the same way as you set up the first connector.

You then associate all the connector instances with the Built-in identity provider. The VMware Identity Manager service automatically distributes traffic among all the connectors associated with the Built-in identity provider. A load balancer is not required. If one of the connectors becomes unavailable because of a network issue, the service does not direct traffic to it. When connectivity is restored, the service resumes sending traffic to the connector.

After you set up the connector cluster, the authentication methods that you enabled on the connector are highly available. If one of the connector instances is unavailable, authentication is still available. 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. Directory sync can only be enabled on one connector at a time.

Note This section does not apply to high availability of Kerberos authentication. See Chapter 5 Adding Kerberos Authentication Support to Your VMware Identity Manager Connector Deployment.

This chapter includes the following topics:

Install Additional Connector Instances

After you install and configure the first connector instance, you can add additional connectors for high availability. Install new connector virtual appliances and configure them in exactly the same way as the first connector instance.

Prerequisites

You have installed and configured the first connector instance, as described in Chapter 3 Deploying the VMware Identity Manager Connector.

Procedure

1 Install and configure a new connector instance by following these instructions.

- Generate Activation Code for Connector
- Install and Configure the Connector Virtual Appliance

2 Associate the new connector with the `WorkspaceIDP` of the first connector instance.

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 `WorkspaceIDP` of the first connector instance and click the link.

c In the **Connector(s)** field, select the new connector.

d Enter the Bind DN password and click **Add Connector**.

e Click **Save**.

3 If you had joined an Active Directory domain in the first connector instance, then you must join the domain in the new connector instance too.

a In the **Identity & Access Management** tab, click **Setup**.

The new connector instance is listed in the Connectors page.

b Click **Join Domain** next to the new connector and specify the domain information.

Note For directories of type Integrated Windows Authentication (IWA), you must perform the following actions.

a Join the new connector instance to the domain to which the IWA directory in the original connector instance was joined.

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

The new connector instance is listed in the Connectors page.

2 Click **Join Domain** and specify the domain information.

b Save the IWA directory configuration.

1 Select the **Identity & Access Management** tab.

2 In the Directories page, click the IWA directory link.

3 Click **Save** to save the directory configuration.

---

4 Configure and enable authentication adapters on the new connector.

Important Authentication adapters on all the connectors in your cluster must be configured identically. The same authentication methods must be enabled on all the connectors.

a In the **Identity & Access Management** tab, click **Setup**, then click the **Connectors** tab.

b Click the link in the **Worker** column of the new connector.

c Click the **Auth Adapters** tab.

All available authentication adapters for the connector are listed.

The PasswordIdpAdapter is already configured and enabled because you associated the new connector with the directory associated with the first connector.

d Configure and enable the other authentication adapters in the same way as the first connector. Ensure that the configuration information is identical.

For information on configuring authentication adapters, see the *VMware Identity Manager Administration Guide*.

What to do next

Add New Connector to Built-in Identity Provider

Add New Connector to Built-in Identity Provider

After you deploy and configure the new connector instance, add it to the Built-in identity provider and enable the same authentication methods that are enabled on the first connector. VMware Identity Manager automatically distributes traffic among all the connectors associated with the Built-in identity provider.

Procedure

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

2 Click the **Identity Providers** tab.

3 Click the **Built-in** link.

4 In the **Connector(s)** field, select the new connector from the drop-down list and click **Add Connector**.

5 In the **Connector Authentication Methods** section, enable the same authentication methods that you selected for the first connector.

The Password (cloud deployment) authentication method is automatically configured and enabled. You must enable the other authentication methods.

Important Authentication adapters on all the connectors in your cluster must be configured identically. The same authentication methods must be enabled on all the connectors.

For information on configuring specific authentication adapters, see the *VMware Identity Manager Administration Guide*.

6 Click **Save** to save the Built-in identity provider configuration.

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

In the event of a connector instance failure, authentication is handled automatically by another connector instance. However, for directory sync, you must 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.

Tip 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** drop-down list, select another connector instance.

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

6 Click **Save**.

Adding Kerberos Authentication Support to Your VMware Identity Manager Connector Deployment

5

You can add Kerberos authentication for internal users, which requires inbound connection mode, to your deployment of outbound connection mode connectors. The same connectors can be configured to use Kerberos authentication for users coming from the internal network and another authentication method for users coming from the external network. This can be achieved by defining authentication policies based on network ranges.

Requirements and considerations include:

- Kerberos authentication can be configured regardless of the type of directory you set up in VMware Identity Manager, Active Directory over LDAP or Active Directory (Integrated Windows Authentication).
- The connector must be joined to the Active Directory domain.
- The connector host name must match the Active Directory domain to which the connector is joined. For example, if the Active Directory domain is sales.example.com, the connector host name must be *connectorhost*.sales.example.com.

  If you cannot assign a hostname that matches the Active Directory domain structure, you need to configure the connector and Active Directory manually. See the Knowledge Base for information.
- Each connector on which Kerberos authentication is configured must have a trusted SSL certificate. You can obtain the certificate from your internal certificate authority. Kerberos authentication does not work with self-signed certificates.

  Trusted SSL certificates are required regardless of whether you enable Kerberos on a single connector or on multiple connectors for high availability.
- To set up high availability for Kerberos authentication, a load balancer is required.

This chapter includes the following topics:

Configuring and Enabling the Kerberos Authentication Adapter

Configure and enable the KerberosIdpAdapter on the VMware Identity Manager Connector. If you have deployed a cluster for high availability, configure and enable the adapter on all the connectors in your cluster.

Important Authentication adapters on all the connectors in your cluster must be configured identically. The same authentication methods must be configured on all the connectors.

For more information about configuring Kerberos authentication, see the *VMware Identity Manager Administration Guide*.

Prerequisites

- The connector must be joined to the Active Directory domain.
- The connector host name must match the Active Directory domain to which the connector is joined. For example, if the Active Directory domain is sales.example.com, the connector host name must be *connectorhost*.sales.example.com.

  If you cannot assign a hostname that matches the Active Directory domain structure, you need to configure the connector and Active Directory manually. See the Knowledge Base for information.

Procedure

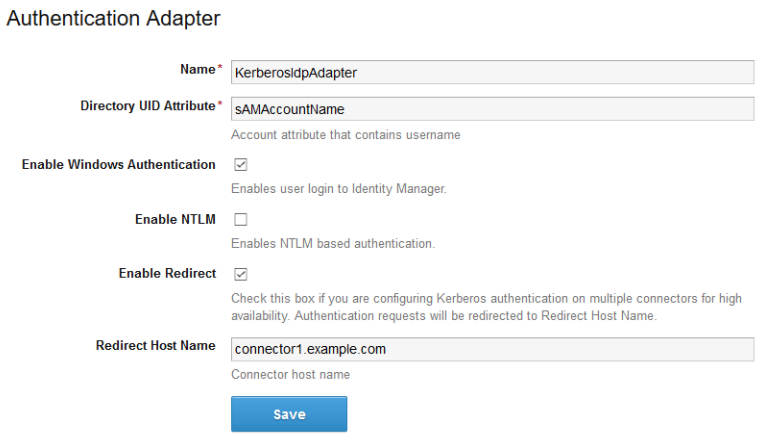
1. In the VMware Identity Manager administration console, click the **Identity & Access Management** tab.
2. Click **Setup**, then click the **Connectors** tab.

   All the connectors that you have deployed are listed.
3. Click the link in the **Worker** column of one of the connectors.
4. Click the **Auth Adapters** tab.
5. Click the KerberosIdpAdapter link, and configure and enable the adapter.

Option	Description
Name	The default name of the adapter is KerberosIdpAdapter. You can change this name.
Directory UID Attribute	The account attribute that contains username.
Enable Windows Authentication	Select this option.
Enable NTLM	You do not need to select this option unless your Active Directory infrastructure relies on NTLM authentication. **Note** This option is only supported on Linux-based VMware Identity Manager.

Option	Description
Enable Redirect	If you have multiple connectors in a cluster and plan to set up Kerberos high availability by using a load balancer, select this option and specify a value for **Redirect Host Name**. If your deployment has only one connector, you do not need to use the **Enable Redirect** and **Redirect Host Name** options.
Redirect Host Name	A value is required if the **Enable Redirect** option is selected. Enter the connector's own host name. For example, if the connector's host name is connector1.example.com, enter **`connector1.example.com`** in the text box.

For example:



For more information on configuring the KerberosIdPAdapter, see the *VMware Identity Manager Administration Guide*.

6 Click **Save**.

7 If you have deployed a cluster, configure the KerberosIdPAdapter on all the connectors in your cluster.

Ensure that you configure the adapter identically on all the connectors, except for the Redirect Host Name value, which should be specific to each connector.

What to do next

- Ensure that each connector on which the KerberosIdpAdapter is enabled has a trusted SSL certificate. You can obtain the certificate from your internal certificate authority. Kerberos authentication does not work with self-signed certificates.

  Trusted SSL certificates are required regardless of whether you enable Kerberos on a single connector or on multiple connectors for high availability.

- Set up high availability for Kerberos authentication, if necessary. Kerberos authentication is not highly available without a load balancer.

Configuring High Availability for Kerberos Authentication

To configure high availability for Kerberos authentication, install a load balancer in your internal network inside the firewall and add the VMware Identity Manager Connector instances to it.

You must also configure certain settings on the load balancer, establish SSL trust between the load balancer and the connector instances, and change the connector authentication URL to use the load balancer host name.

Configure Load Balancer Settings

You must configure certain settings on the load balancer, such as setting the load balancer timeout correctly and enabling sticky sessions.

Configure these settings.

- Load Balancer Timeout

  For the VMware Identity Manager 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 the following 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 instances. The load balancer will then bind a user's session to a specific connector instance.

Apply VMware Identity Manager Connector Root Certificate to the Load Balancer

When the VMware Identity Manager Connector is configured behind a load balancer, you must establish SSL trust between the load balancer and the connector. The connector root certificate must be copied to the load balancer as a trusted root certificate.

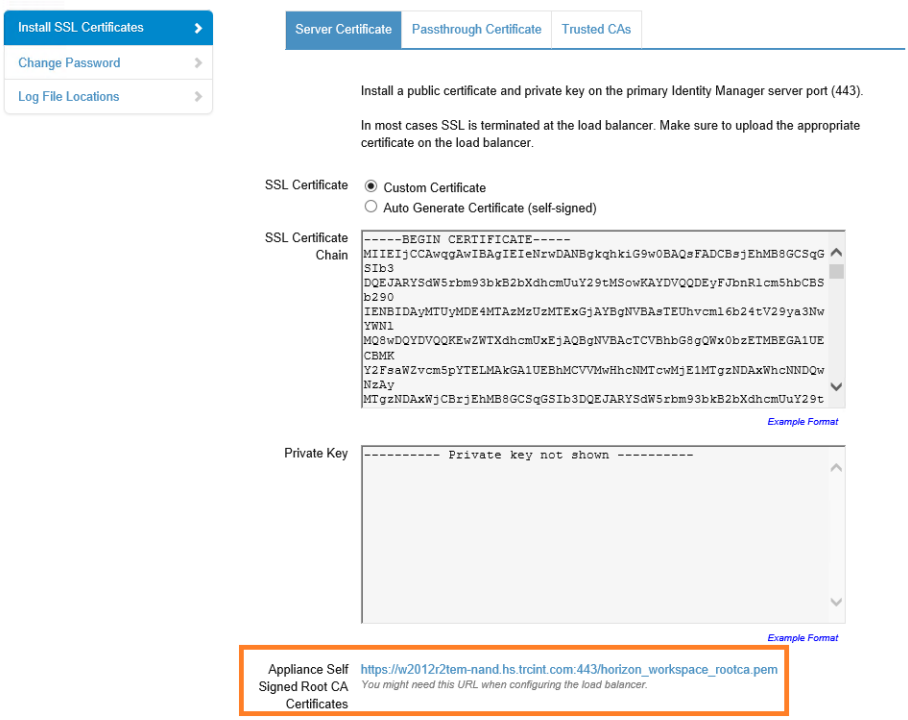
The VMware Identity Manager Connector certificate can be downloaded from the connector admin pages at https://*connectorFQDN*:8443/cfg/ssl.

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

Procedure

1. Log in to the connector admin pages, https://*connectorFQDN*:8443/cfg/login, as the admin user.
2. Select **Install SSL Certificates**.

3 In the **Server Certificate** tab, click the link in the **Appliance Self Signed Root CA Certificates** field.



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 load balancer documentation.

What to do next

Copy and paste the load balancer root certificate to the VMware Identity Manager Connector.

Apply Load Balancer Root Certificate to the VMware Identity Manager Connector

When the VMware Identity Manager Connector is configured behind a load balancer, you must establish trust between the load balancer and the connector. In addition to copying the connector root certificate to the load balancer, you must copy the load balancer root certificate to the connector.

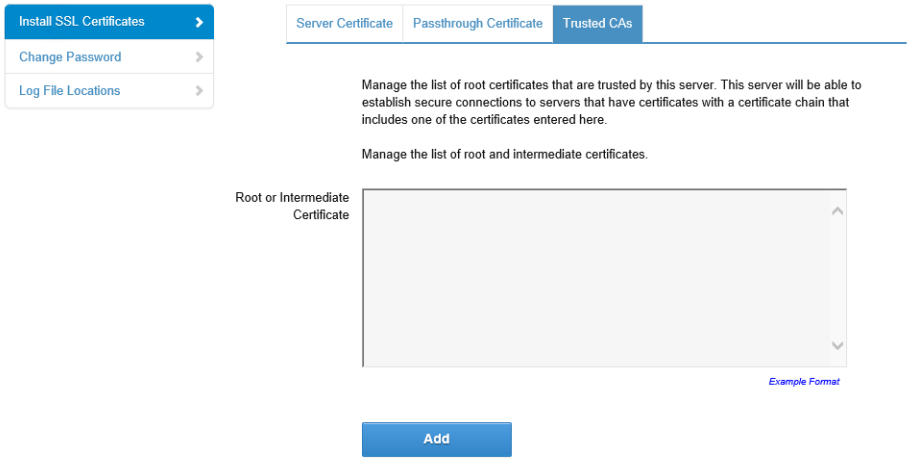
Procedure

1 Obtain the load balancer root certificate.

2 Go to the VMware Identity Manager Connector admin pages at https://*connectorFQDN*:8443/cfg/login and log in as the admin user.

3 Select the **Install SSL Certificates > Trusted CAs** tab.

4 Paste the text of the load balancer certificate into the **Root or Intermediate Certificate** text box.



5 Click **Add**.

Change Connector IdP Host Name to the Load Balancer Host Name

After you add the VMware Identity Manager Connector instances to the load balancer, you must change the IdP host name on the Workspace IdP of each connector to the load balancer host name.

Prerequisites

The connector instances are configured behind a load balancer. Make sure that the load balancer port is 443. Do not use 8443 as this port number is the administrative port.

Procedure

1 Log in to the VMware Identity Manager administration console.

2 Click the **Identity & Access Management** tab.

3 Click the **Identity Providers** tab.

4 In the Identity Providers page, click the Workspace IdP link for the connector instance.

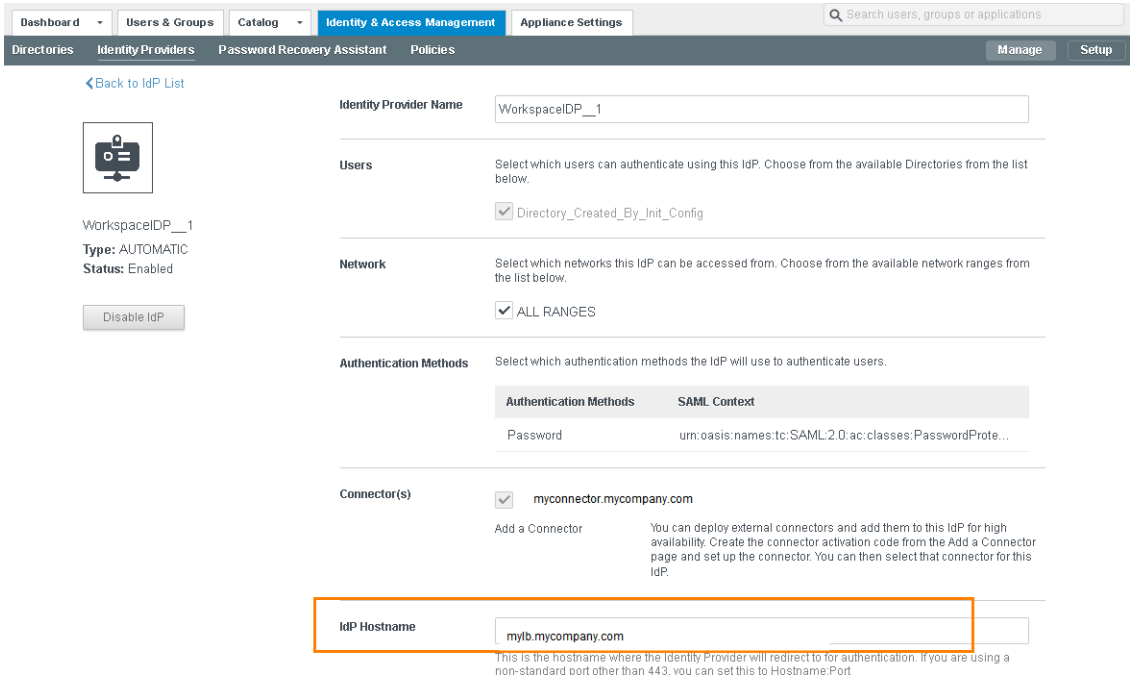
5 In the **IdP Hostname** text box, change the host name from the connector host name to the load balancer host name.

For example, if your connector host name is `myconnector` and your load balancer hostname is `mylb`, change the URL

```
myconnector.mycompany.com:port
```

to the following:

```
mylb.mycompany.com:port
```



Integrating Your Enterprise Directory with VMware Identity Manager

6

You integrate your enterprise directory with VMware Identity Manager 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 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.

This chapter includes the following topics:

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.

VMware Identity Manager Connector

The VMware Identity Manager Connector is an on premises component 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 VMware Identity Manager service.
- When being used as an identity provider, authenticates users to theVMware Identity Manager 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.

Security Considerations

For enterprise directories integrated with the VMware Identity Manager service, security settings such as user password complexity rules and account lockout policies must be set in the enterprise directory directly. VMware Identity Manager does not override these settings.

Integrating with Active Directory

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.

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)
- Managing User Attributes that Sync from Active Directory
- Permissions Required for Joining a Domain (Linux Virtual Appliance Only)
- Configuring Active Directory Connection to the Service

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)
  - Managing User Attributes that Sync from Active Directory
  - Permissions Required for Joining a Domain (Linux Virtual Appliance Only)
  - Configuring Active Directory Connection to the Service

- 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.
  - When AirWatch is integrated with VMware Identity Manager and multiple AirWatch organization groups are configured, the Active Directory Global Catalog option cannot be used.

  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)
- Managing User Attributes that Sync from Active Directory
- Permissions Required for Joining a Domain (Linux Virtual Appliance Only)
- Configuring Active Directory Connection to the Service

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)
- Managing User Attributes that Sync from Active Directory
- Permissions Required for Joining a Domain (Linux Virtual Appliance Only)
- Configuring Active Directory Connection to the Service

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.

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 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.

  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.

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 some 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).

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 select 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 attributes that you want to sync to the directory. When you add attributes, 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.

The following attributes cannot be used as custom attribute names because VMware Identity Manager service uses these attributes internally for user identity management.

- externalUserDisabled
- employeeNumber

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 not to be required, and you can delete custom attributes. You cannot change an attribute to be a required attribute.

Procedure

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

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

3 Click **Save**.

Permissions Required for Joining a Domain (Linux Virtual Appliance Only)

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, unless you specify a custom OU.

If you do not have the rights to join a domain, 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**.

Option	Description
Domain	Select or enter the Active Directory domain to join. Ensure that you enter the fully-qualified domain name. For example, **server.example.com**.
Domain User	The username of an Active Directory user who has the rights to join systems to the Active Directory domain.
Domain Password	The password of the user.
Organizational unit (OU)	(Optional) The organizational unit (OU) of the computer object. This option creates a computer object in the specified OU instead of the default Computers OU. For example, **ou=testou,dc=test,dc=example,dc=com**.

Important This topic applies only to the VMware Identity Manager service and connector Linux virtual appliances. It does not apply to the VMware Identity Manager service or connector on Windows.

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 Active Directory over LDAP or 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 which attributes are required and add additional attributes, if necessary, on the User Attributes page. See Select Attributes to Sync with Directory.
- List of the Active Directory users and groups to sync from Active Directory. Group names are synced to the directory immediately. Members of a group do not sync until the group is entitled to resources or added to a policy rule. Users who need to authenticate before group entitlements are configured should be added during the initial configuration.
- 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) . ■ 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. ■ 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.

Option	Description
	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**. 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 (Linux Virtual Appliance Only) 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 and make changes, if necessary, then click **Next**.

8 Select the groups you want to sync from Active Directory to the VMware Identity Manager directory.

When groups are added here, group names are synced to the directory. Users that are members of the group are not synced to the directory until the group is entitled to an application or the group name is added to an access policy rule. Any subsequent scheduled syncs bring updated information from Active Directory for these group names.

Option	Description
Specify the group DNs	To select groups, you specify one or more group DNs and select the groups under them. a Click **+** and specify the group DN. For example, CN=users,DC=example,DC=company,DC=com. **Important** Specify group DNs that are under the Base DN that you entered. If a group DN is outside the Base DN, users from that DN will be synced but will not be able to log in. b Click **Find Groups**. The **Groups to Sync** column lists the number of groups found in the DN. c To select all the groups in the DN, click **Select All**, otherwise click **Select** and select the specific groups 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.
Sync nested group members	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 when the group is entitled. 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 parent group that you selected for sync. If the **Sync nested group members** 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.

9 Click **Next**.

10 Specify additional users to sync, if required.

Because members in groups do not sync to the directory until the group is entitled to applications or added to an access policy rule, add all users who need to authenticate before group entitlements are configured.

a Click **+** and enter the user DNs. For example, CN=username,CN=Users,OU=myUnit,DC=myCorp,DC=com.

Important Specify user DNs that are under the Base DN that you entered. If a user DN is outside the Base DN, users from that DN will be synced but will not be able to log in.

b (Optional) 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.

11 Click **Next**.

12 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.

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

The connection to Active Directory is established and users and group names 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.

For more information about how groups are synced, see "Managing Users and Groups" in *VMware Identity Manager Administration*.

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).
- Set up authentication methods. After users and group names 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.
- Review the default access policy. The default access policy is configured to allow all appliances in all network ranges to access the portal, with a session time out set to eight hours or to access a client app with a session time out of 2160 hours (90 days). You can change the default access policy and create new ones.

Enabling Users to Change Active Directory Passwords

You can provide users the ability to change their Active Directory passwords from the Workspace ONE portal or app whenever they want. Users can also reset 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 enable this option per directory, by selecting the **Allow Change Password** option in the Directory Settings page.

Users can change their passwords when they are logged into the Workspace ONE portal by clicking their name in the top-right corner, selecting **Account** from the drop-down menu, and clicking the **Change Password** link. In the Workspace ONE app, users can change their passwords by clicking the triple-bar menu icon and selecting **Password**.

Expired passwords or passwords reset by the administrator in Active Directory can be changed from the login 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.

The following limitations apply.

- The Active Directory Domain functional level must be set to Windows 2008 or later.
- When a directory is added to VMware Identity Manager as a Global Catalog, the **Allow Change Password** option is not available. Directories can be added as Active Directory over LDAP or Integrated Windows Authentication, using ports 389 or 636.
- 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.

Note The Allow Change Password option cannot be enabled for ACC directories.

Prerequisites

- Port 464 must be open from VMware Identity Manager to the domain controllers. In a SaaS deployment, port 464 must be open from the VMware Identity Manager connector to the domain controllers.
- The **Allow Change Password** option is only available with connector version 2016.11.1 and later.

Procedure

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

2 In the **Directories** tab, click the directory.

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

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

Integrating with LDAP Directories

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.

See also Important Concepts Related to Directory Integration.

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 Horizon 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.

Integrating 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 the 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 might be based on default schemas or custom schemas. It may also have 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.

Prerequisites

- Review the attributes in the **Identity & Access Management > Setup > User Attributes** page and add additional attributes that you want to sync. You map the VMware Identity Manager attributes to your LDAP directory attributes 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** text box, select the connector you want to use to sync users and groups from your LDAP directory to the VMware Identity Manager directory. In an on premises deployment, 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 instances for high availability, the connector component of each appears in the list. Additional, external connectors are also listed. You do not need to use a separate connector for an LDAP directory. A connector can support multiple directories, regardless of whether they are Active Directory or LDAP directories. For the scenarios in which you need additional connectors, see *Installing and Configuring VMware Identity Manager*. b In the **Authentication** text box, 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** text box, 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.

Option	Description
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`
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.

These attributes will be synced for users.

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.

When groups are added, group names are synced to the directory. Users that are members of the group are not synced to the directory until the group is entitled to an application or the group name is added to an access policy rule.

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 when the group is entitled. 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 users. For example, enter **`CN=username,CN=Users,OU=myUnit,DC=myCorp,DC=com`**.

Because members in groups do not sync to the directory until the group is entitled to applications or added to an access policy rule, add all users who need to authenticate before group entitlements are configured.

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 group names 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 group names 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.

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 (Optional) If you are using a load balancer, in the **IdP Hostname** field, enter the load balancer FQDN, if it is not already set to the correct load balancer FQDN.

Note This step is required only if you are using a load balancer. You do not need to use a load balancer with the connector in outbound-only connection mode. However, you may have set up a load balancer for certain scenarios such as Kerberos authentication.

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

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

7 (Optional) If you are using a load balancer, in the Identity Providers page, click the Identity Provider name again and verify that the **IdP Hostname** field displays the load balancer FQDN. If the name is incorrect, enter the load balancer FQDN and click **Save**.

Note This step is required only if you are using a load balancer.

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

Note If you are using a load balancer, 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.

Using Local Directories

7

A local directory is one of the types of directories that you can create in the VMware Identity Manager service. A local directory enables you to provision local users in the service and provide them access to specific applications, without having to add them to your enterprise directory. A local directory is not connected to an enterprise directory and users and groups are not synced from an enterprise directory. Instead, you create local users directly in the local directory.

A default local directory, named System Directory, is available in the service. You can also create multiple new local directories.

System Directory

The System Directory is a local directory that is automatically created in the service when it is first set up. This directory has the domain System Domain. You cannot change the name or domain of the System Directory, or add new domains to it. Nor can you delete the System Directory or the System Domain.

A local administrator user is created in the System Domain of the System Directory when the tenant is first set up. The credentials you receive when you get a new tenant belong to this local administrator user.

You can add other users to the System Directory. The System Directory is typically used to set up a few local administrator users to manage the service. To provision end users and additional administrators and entitle them to applications, creating a new local directory is recommended.

Local Directories

You can create multiple local directories. Each local directory can have one or more domains. When you create a local user, you specify the directory and domain for the user.

You can also select attributes for all the users in a local directory. User attributes such as userName, lastName, and firstName are specified at the global level in the VMware Identity Manager service. A default list of attributes is available and you can add custom attributes. Global user attributes apply to all directories in the service, including local directories. At the local directory level, you can select which attributes are required for the directory. This allows you to have a custom set of attributes for different local directories. Note that userName, lastName, firstName, and email are always required for local directories.

Note The ability to customize user attributes at the directory level is only available for local directories, not for Active Directory or LDAP directories.

Creating local directories is useful in scenarios such as the following.

- You can create a local directory for a specific type of user that is not part of your enterprise directory. For example, you can create a local directory for partners, who are not usually part of your enterprise directory, and provide them access to only the specific applications they need.
- You can create multiple local directories if you want different user attributes or authentication methods for different sets of users. For example, you can create a local directory for distributors that has user attributes such as region and market size, and another local directory for suppliers that has user attributes such as product category and supplier type.

Identity Provider for System Directory and Local Directories

By default, the System Directory is associated with an identity provider named System Identity Provider. The Password (Cloud Directory) method is enabled by default on this identity provider and applies to the default_access_policy_set policy for the ALL RANGES network range and the Web Browser device type. You can configure additional authentication methods and set authentication policies.

When you create a new local directory, it is not associated with any identity provider. After creating the directory, create a new identity provider of type Embedded and associate the directory with it. Enable the Password (Cloud Directory) authentication method on the identity provider. Multiple local directories can be associated with the same identity provider.

The VMware Identity Manager connector is not required for either the System Directory or for local directories you create.

For more information, see "Configuring User Authentication in VMware Identity Manager" in *VMware Identity Manager Administration*.

Password Management for Local Directory Users

By default, all users of local directories have the ability to change their password in the Workspace ONE portal or app. You can set a password policy for local users. You can also reset local user passwords as needed.

Users can change their passwords when they are logged into the Workspace ONE portal by clicking their name in the top-right corner, selecting **Account** from the drop-down menu, and clicking the **Change Password** link. In the Workspace ONE app, users can change their passwords by clicking the triple-bar menu icon and selecting **Password**.

For information on setting password policies and resetting local user passwords, see "Managing Users and Groups" in *VMware Identity Manager Administration*.

This chapter includes the following topics:

Creating a Local Directory

To create a local directory, you specify the user attributes for the directory, create the directory, and identify it with an identity provider.

Set User Attributes at the Global Level

Before you create a local directory, review the global user attributes on the User Attributes page and add custom attributes, if necessary.

User attributes, such as firstName, lastName, email and domain, are part of a user's profile. In the VMware Identity Manager service, user attributes are defined at the global level and apply to all directories in the service, including local directories. At the local directory level, you can override whether an attribute is required or optional for users in that local directory, but you cannot add custom attributes. If an attribute is required, you must provide a value for it when you create a user.

The following words cannot be used when you create custom attributes.

Table 7-1. Words that cannot be used as Custom Attribute Names

active	addresses	costCenter
department	displayName	division
emails	employeeNumber	entitlements
externalId	groups	id
ims	locale	manager
meta	name	nickName
organization	password	phoneNumber
photos	preferredLanguage	profileUrl

Table 7-1. Words that cannot be used as Custom Attribute Names (Continued)

roles	timezone	title
userName	userType	x509Certificate

Note The ability to override user attributes at the directory level only applies to local directories, not to Active Directory or LDAP directories.

Procedure

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

2 Click **Setup**, then click the **User Attributes** tab.

3 Review the list of user attributes and add additional attributes, if necessary.

Note Although this page lets you select which attributes are required, it is recommended that you make the selection for local directories at the local directory level. If an attribute is marked required on this page, it applies to all directories in the service, including Active Directory or LDAP directories.

4 Click **Save**.

What to do next

Create the local directory.

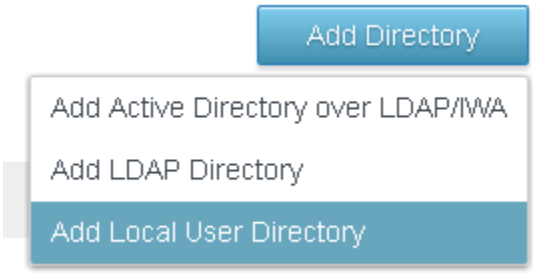
Create a Local Directory

After you review and set global user attributes, create the local directory.

Procedure

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

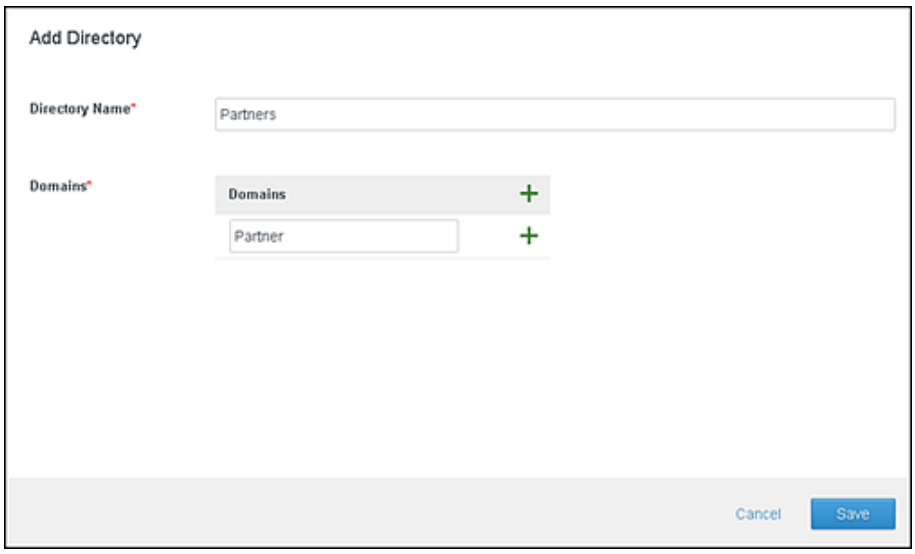
2 Click **Add Directory** and select **Add Local User Directory** from the drop-down menu.



3 In the Add Directory page, enter a directory name and specify at least one domain name.

The domain name must be unique across all directories in the service.

For example:



4 Click **Save**.

5 In the Directories page, click the new directory.

6 Click the **User Attributes** tab.

All the attributes from the Identity & Access Management > Setup > User Attributes page are listed for the local directory. Attributes that are marked required on that page are listed as required in the local directory page too.

7 Customize the attributes for the local directory.

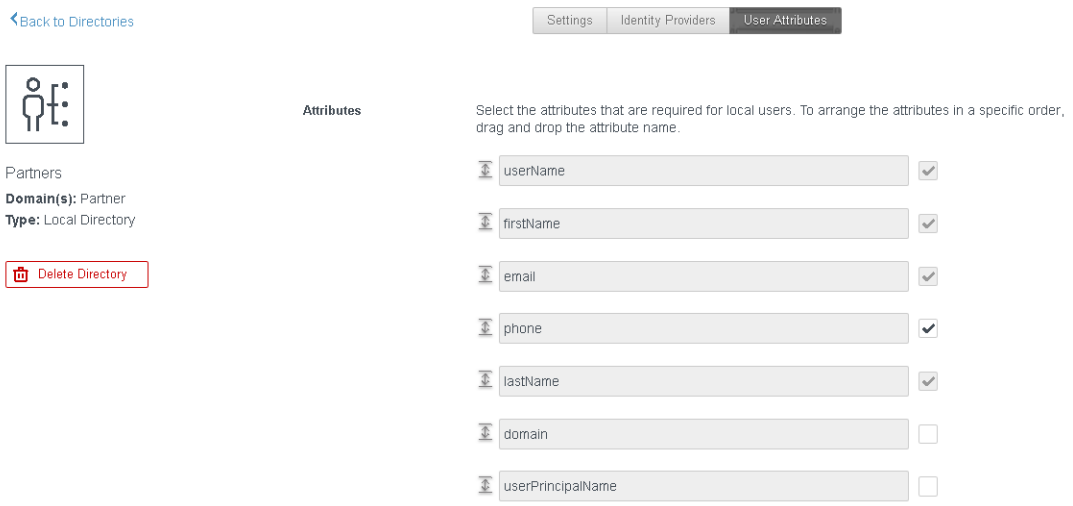
You can specify which attributes are required and which attributes are optional. You can also change the order in which the attributes appear.

Important The attributes userName, firstName, lastName, and email are always required for local directories.

- To make an attribute required, select the check box next to the attribute name.
- To make an attribute optional, deselect the check box next to the attribute name.
- To change the order of the attributes, click and drag the attribute to the new position.

If an attribute is required, when you create a user you must specify a value for the attribute.

For example:



8 Click **Save**.

What to do next

Associate the local directory with the identity provider you want to use to authenticate users in the directory.

Associate the Local Directory With an Identity Provider

Associate the local directory with an identity provider so that users in the directory can be authenticated. Create a new identity provider of type Embedded and enable the Password (Local Directory) authentication method on it.

Note Do not use the Built-in identity provider. Enabling the Password (Local Directory) authentication method on the Built-in identity provider is not recommended.

Prerequisites

The Password (Local Directory) authentication method must be configured in the Identity & Access Management > Authentication Methods page.

Procedure

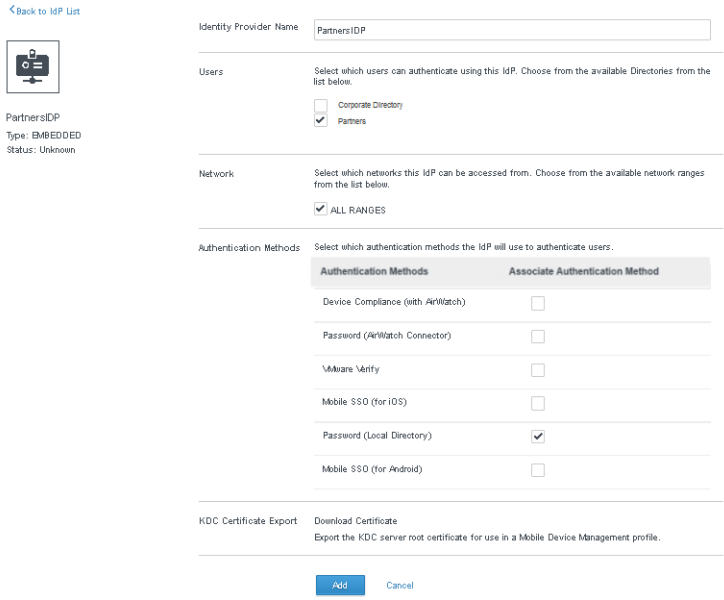
1 In the **Identity & Access Management** tab, click the **Identity Providers** tab.

2 Click **Add Identity Provider** and select **Create Built-in IDP**.

3 Enter the following information.

Option	Description
Identity Provider Name	Enter a name for the identity provider.
Users	Select the local directory you created.
Network	Select the networks from which this identity provider can be accessed.

Option	Description
Authentication Methods	Select Password (Local Directory).
KDC Certificate Export	You do not need to download the certificate unless you are configuring mobile SSO for AirWatch-managed iOS devices.



4 Click **Add**.

The identity provider is created and associated with the local directory. Later, you can configure other authentication methods on the identity provider. For more information about authentication, see "Configuring User Authentication in VMware Identity Manager" in *VMware Identity Manager Administration*.

You can use the same identity provider for multiple local directories.

What to do next

Create local users and groups. You create local users and groups in the **Users & Groups** tab in the administration console. See "Managing Users and Groups" in *VMware Identity Manager Administration* for more information.

Changing Local Directory Settings

After you create a local directory, you can modify its settings at any time.

You can change the following settings.

- Change the directory name.
- Add, delete, or rename domains.
  - Domain names must be unique across all directories in the service.
  - When you change a domain name, the users that were associated with the old domain are associated with the new domain.

  - The directory must have at least one domain.
  - You cannot add a domain to the System Directory or delete the System Domain.
- Add new user attributes or make an existing attribute required or optional.
  - If the local directory does not have any users yet, you can add new attributes as either optional or required, and change existing attributes to required or optional.
  - If you have already created users in the local directory, you can add new attributes as optional attributes only, and change existing attributes from required to optional. You cannot make an optional attribute required after users have been created.
  - The attributes userName, firstName, lastName, and email are always required for local directories.
  - As user attributes are defined at the global level in the VMware Identity Manager service, any new attributes you add will appear in all directories in the service.
- Change the order in which attributes appear.

Procedure

1. Click the **Identity & Access Management** tab.
2. In the Directories page, click the directory you want to edit.
3. Edit the local directory settings.

Option	Action
Change the directory name	a In the **Settings** tab, edit the directory name. b Click **Save**.
Add, delete, or rename a domain	a In the **Settings** tab, edit the **Domains** list. b To add a domain, click the green plus icon. c To delete a domain, click the red delete icon. d To rename a domain, edit the domain name in the text box.
Add user attributes to the directory	a Click the **Identity & Access Management** tab, then click **Setup**. b Click the **User Attributes** tab. c Add attributes in the **Add other attributes to use** list, and click **Save**.
Make an attribute required or optional for the directory	a In the **Identity & Access Management** tab, click the **Directories** tab. b Click the local directory name and click the **User Attributes** tab. c Select the check box next to an attribute to make it a required attribute, or deselect the check box to make it an optional attribute. d Click **Save**.
Change the order of the attributes	a In the **Identity & Access Management** tab, click the **Directories** tab. b Click the local directory name and click the **User Attributes** tab. c Click and drag the attributes to the new position. d Click **Save**.

Deleting a Local Directory

You can delete a local directory that you created in the VMware Identity Manager service. You cannot delete the System Directory, which is created by default when you first set up the service.

Caution When you delete a directory, all users in the directory are also deleted from the service.

Procedure

1. Click the **Identity & Access Management** tab, then click the **Directories** tab.
2. Click the directory you want to delete.
3. In the directory page, click **Delete Directory**.

Managing VMware Identity Manager Connector Admin Settings

8

After the initial VMware Identity Manager connector configuration is complete, you can go to the connector admin pages at any time to install certificates, manage passwords, and download log files.

The VMware Identity Manager Connector admin pages are available at https://*connectorFQDN*:8443/cfg/login, for example, https://myconnector.example.com:8443/cfg/login. Log in as the connector admin user with the admin password you created when you installed the connector.

Table 8-1. Connector Settings

Option	Description
Install SSL Certificates	On the tabs on this page, you can install an SSL certificate for the connector, download the self-signed root certificate, and install trusted root certificates. **Note** The **Passthrough Certificate** tab is used only when certificate authentication is configured on the embedded connector in a DMZ deployment scenario. It is not applicable in any other scenarios. See *Deploying VMware Identity Manager in the DMZ* for information.
Configure Syslog	On this page, you can enable an external syslog server if you want connector logs to be sent to the external server.
Change Password	On this page, you can change the connector admin password.
System Security	On this page, you can change the root and ssh user passwords for the connector.
Log File Locations	On this page, you can create and download a bundle of connector log files.

This chapter includes the following topics:

Using SSL Certificates for the Connector

When the VMware Identity Manager connector is installed, a default self-signed SSL server certificate is automatically generated. You can continue to use this self-signed certificate in most scenarios.

With the connector deployed in outbound mode, end users do not access the connector directly, so installing a public Certificate Authority (CA)-signed SSL certificate is not required. For administrator access to the connector, you can either continue to use the default self-signed certificate or use a certificate generated by your internal CA.

However, if you enable the KerberosIdpAdapter on the connector to set up Kerberos authentication for internal users, end users will establish SSL connections to the connector so the connector must have a signed SSL certificate. Use your internal CA to generate the SSL certificate.

If you set up high availability for Kerberos authentication, a load balancer is required in front of the connector instances. In this case, the load balancer as well as all the connector instances must have signed SSL certificates. Use your internal CA to generate the SSL certificates. For the load balancer certificate, use the Workspace IdP Hostname, which is set in the Workspace IdP configuration page, as the Subject DN Common Name. For each connector instance certificate, use the connector host name as the Subject DN Common Name. Alternatively, you can create a single certificate, using the Workspace Idp host name as the Subject DN Common Name, and all the connector host names as well as the Workspace Idp host name as Subject Alternative Names (SANs).

Installing a Signed SSL Certificate for the Connector

You can install a signed SSL certificate for the VMware Identity Manager connector from the connector admin pages at https://*connectorFQDN*:8443/cfg/login.

See Using SSL Certificates for the Connector for the scenarios in which a signed SSL certificate is required.

Prerequisites

Generate a Certificate Signing Request (CSR) and obtain a signed SSL certificate. The certificate must be in the PEM format.

Procedure

1. Log in to the connector admin pages at https://*connectorFQDN*:8443/cfg/login as the admin user.
2. Click **Install SSL Certificates**.
3. In the **Server Certificate** tab, for the **SSL Certificate** field select **Custom Certificate**.
4. In the **SSL Certificate Chain** text box, paste the server, intermediate, and root certificates, in that order.

   You must include the entire certificate chain in the correct order. For each certificate, copy everything between and including the lines -----BEGIN CERTIFICATE----- and -----END CERTIFICATE-----.

5 In the **Private Key** text box, paste the private key. Copy everything between ----BEGIN RSA PRIVATE KEY and ---END RSA PRIVATE KEY.

6 Click **Add**.

Example: Certificate Examples

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

Downloading the Connector Self-Signed Root CA Certificate

If you deploy the connector with the self-signed SSL certificate that is generated by default when the connector is installed, install the connector's self-signed root CA certificate on any clients that access the connector. You can download the root CA certificate from the VMware Identity Manager administration console.

Procedure

1 Log in to the VMware Identity Manager connector admin pages at https://*connectorFQDN*:8443/cfg/login as the admin user.

2 Click **Install SSL Certificates**.

3 In the **Server Certificate** tab, click the link in the **Appliance Self-Signed Root CA Certificates** field.

The certificates are displayed.

4 Copy the entire text, including the lines `-----BEGIN CERTIFICATE-----` and `-----END CERTIFICATE-----`.

Installing Trusted Root Certificates on the Connector

Install the root or intermediate certificates that should be trusted by the VMware Identity Manager connector. The connector will be able to establish secure connections to servers whose certificate chain includes any of these certificates.

Scenarios in which you need to install trusted root certificates on the connector include the following:

- If you have set up a load balancer for high availability of Kerberos authentication, install the load balancer's root CA certificate on the connector instances to establish trust between the connectors and the load balancer.
- If you have integrated Citrix published resources, install the Integration Broker's SSL certificate on the connectors that will communicate with the Integration Broker.

Procedure

1 Log in to the connector admin pages at https://*connectorFQDN*:8443/cfg/login as the admin user.

2 Click **Install SSL Certificates**, then select the **Trusted CAs** tab.

3 Paste the root or intermediate certificate into the text box.

Include everything between and including the lines -----BEGIN CERTIFICATE----- and -----END CERTIFICATE----.

4 Click **Add.**

Configure a Syslog Server for the Connector

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 did 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.

- Ensure that the connector can reach the syslog server on port 514 (UDP).

Procedure

1. Log in to the connector appliance admin pages at https://*connectorFQDN*: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.

Managing Your VMware Identity Manager Connector Passwords

When you set up the VMware Identity Manager Connector, you created passwords for the admin user, root user, and sshuser. You can change these passwords from the connector admin pages.

Important 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 admin pages at https://*connectorFQDN*:8443/cfg/login as the admin user.
2. Click **Change Password**.
3. Enter the old and new passwords.

   Important The admin user password must be at least 6 characters in length.
4. Click **Save**.
5. To change the root or sshuser passwords, select **System Security**, enter the new passwords, and click **Save**.

Viewing Log Files

The VMware Identity Manager Connector log files can help you debug and troubleshoot problems. The log files can be found in the `/opt/vmware/horizon/workspace/logs` directory in the connector virtual appliance.

The following log files are the most relevant.

Table 8-2. Log Files

Component	Log File Location in a Connector Virtual Appliance	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.

You can also download a log file bundle from the VMware Identity Manager Connector admin pages.

Download a Log Bundle

You can download a log file bundle for the VMware Identity Manager Connector from the connector admin pages. The log files can help you debug and troubleshoot problems.

To collect logs from each connector instance in your environment, log in to the admin pages for each instance.

Procedure

1. Log in to the VMware Identity Manager Connector admin pages at https://*connectorFQDN*:8443/cfg/login as the admin user.
2. Click **Log File Locations** and click **Prepare log bundle**.

   The information is collected into a tar.gz file for you to download.
3. Download the log bundle.

Setting the VMware Identity Manager Connector Log Level to DEBUG

You can set the log level to DEBUG to log additional information that can help debug problems.

Procedure

1. Log in to the virtual appliance.
2. Change to the `/usr/local/horizon/conf/` directory.

3 Update the log level in the `cfg-log4j.properties` and `hc-log4j.properties` files, which are the most commonly-used `log4j` files for the connector.

   a Edit the file.

   b In the lines that have the log level set to `INFO`, replace `INFO` with `DEBUG`.

      For example, change:

      `rootLogger.level=INFO`

      to:

      `rootLogger.level=DEBUG`

   c Save the file.

      A restart of the service or system is not required.

Modifying the Connector URL

You can change the connector URL by updating the identity provider hostname in the administration console.

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**.

Deleting a VMware Identity Manager Connector Instance

9

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 choose to delete a connector instance when you want to use the same host name for a new connector instance, for example.

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 you want to delete, delete the directory first.
   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**.

   The connector instance is deleted from the VMware Identity Manager service.
5. (Optional) Delete the connector virtual appliance.
   a. Log in to the 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**.