Installing and Configuring VMware Identity Manager

VMware Identity Manager 2.8

This document supports the version of each product listed and supports all subsequent versions until the document is replaced by a new edition. To check for more recent editions of this document, see http://www.vmware.com/support/pubs.

EN-002298-01

vmware®

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

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

The VMware Web site also provides the latest product updates.

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

docfeedback@vmware.com

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

Contents

About Installing and Configuring VMware Identity Manager

Installing and Configuring VMware Identity Manager provides information about the installation and configuration process for the VMware Identity Manager appliance. When the installation is finished, you can use the administration console to entitle users to managed multi-device access to your organization's applications, including Windows applications, software as a service (SaaS) applications, and View or Horizon desktops. The guide also explains how to configure your deployment for high availability.

Intended Audience

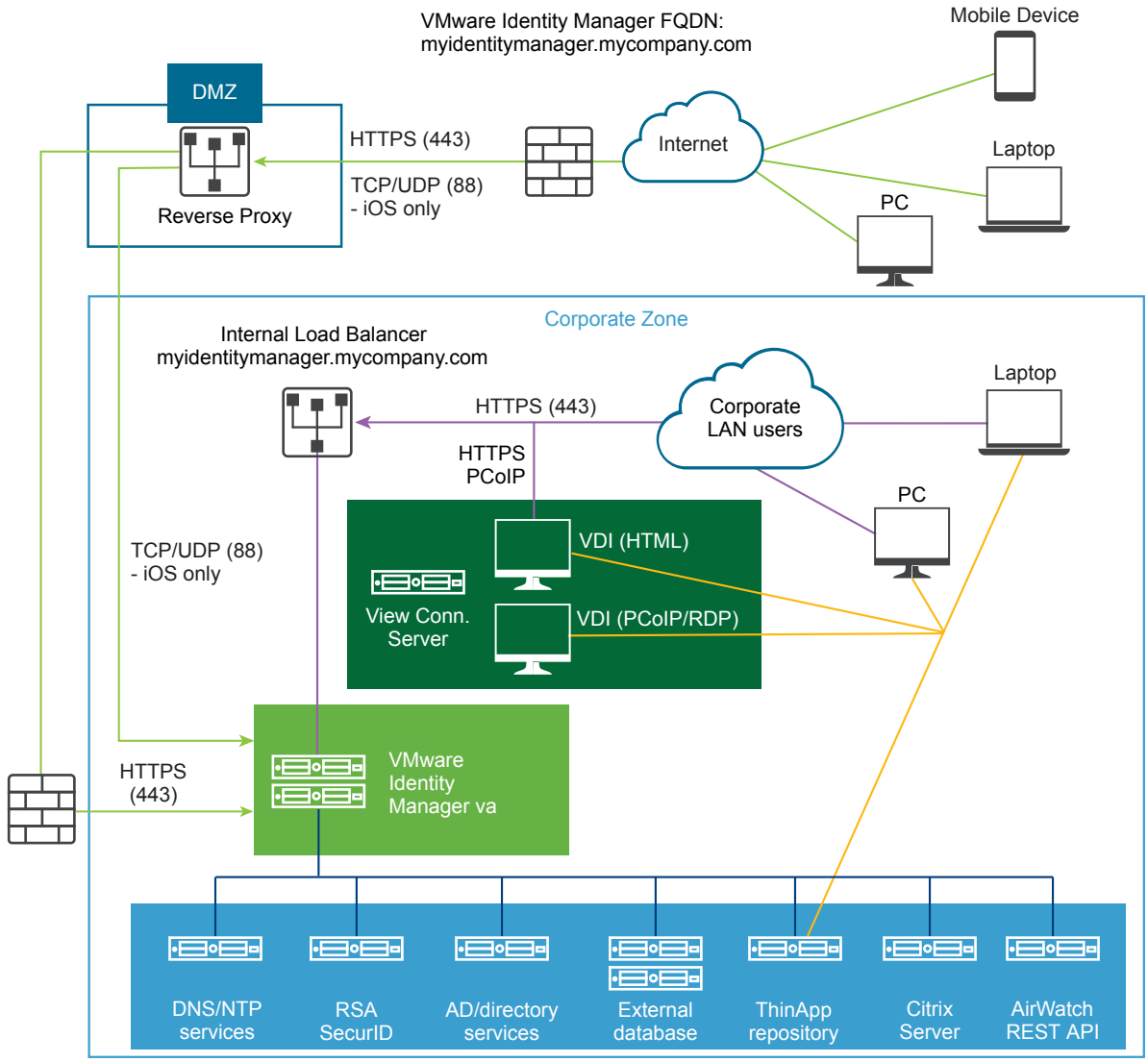
This information is intended for administrators of VMware Identity Manager. The information is written for experienced Windows and Linux system administrators who are familiar with VMware technologies, particularly vCenter™, ESX™, vSphere®, and View™, networking concepts, Active Directory servers, databases, backup and restore procedures, Simple Mail Transfer Protocol (SMTP), and NTP servers. SUSE Linux 11 is the underlying operating system for the virtual appliance. Knowledge of other technologies, such as VMware ThinApp® and RSA SecurID is helpful if you plan to implement those features.

Preparing to Install VMware Identity Manager

1

The tasks to deploy and set up VMware Identity Manager require that you complete the prerequisites, deploy the VMware Identity Manager OVA file and complete the setup from the VMware Identity Manager Setup wizard.

Figure 1-1. VMware Identity Manager Architecture Diagram for Typical Deployments



Note If you plan to enable certificate or smart card-based authentication, use the SSL pass-through setting at the load balancer, instead of the terminate SSL setting. This configuration ensures that the SSL handshake is between the connector, a component of VMware Identity Manager, and the client.

Note Depending on the location of the AirWatch deployment, the AirWatch REST APIs could be in the cloud or on premises.

This chapter includes the following topics:

System and Network Configuration Requirements

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

Supported vSphere and ESX Versions

The following versions of vSphere and ESX server are supported:

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

Note You must turn on time sync at the ESX host level using an NTP server. Otherwise, a time drift occurs between the virtual appliances.

If you deploy multiple virtual appliances on different hosts, consider disabling the Sync to Host option for time synchronization and configuring the NTP server in each virtual appliance directly to ensure that there is no time drift between the virtual appliances.

Hardware Requirements

Ensure that you meet the requirements for the number of VMware Identity Manager virtual appliances and the resources allocated to each appliance.

Number of Users	Up to 1,000	1,000-10,000	10,000-25,000	25,000-50,000	50,000-100,000
Number of VMware Identity Manager servers	1 server	3 load-balanced servers	3 load-balanced servers	3 load-balanced servers	3 load-balanced servers
CPU (per server)	2 CPU	2 CPU	4 CPU	8 CPU	8 CPU
RAM (per server)	6 GB	6 GB	8 GB	16 GB	32 GB
Disk space (per server)	60 GB	100 GB	100 GB	100 GB	100 GB

If you install additional, external connector virtual appliances, ensure that you meet the following requirements.

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
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

Database Requirements

Set up VMware Identity Manager with an external database to store and organize server data. An internal PostgreSQL database is embedded in the virtual appliance but it is not recommended for use with production deployments.

For information about the database versions and service pack configurations supported, see the VMware Product Interoperability Matrices at https://www.vmware.com/resources/compatibility/sim/interop_matrix.php.

The following requirements apply to an external SQL Server database.

Number of Users	Up to 1,000	1,000-10,000	10,000-25,000	25,000-50,000	50,000-100,000
CPU	2 CPU	2 CPU	4 CPU	8 CPU	8 CPU
RAM	4 GB	4 GB	8 GB	16 GB	32 GB
Disk space	50 GB	50 GB	50 GB	100 GB	100 GB

Network Configuration Requirements

Component	Minimum Requirement
DNS record and IP address	IP address and DNS record
Firewall port	Ensure that the inbound firewall port 443 is open for users outside the network to the VMware Identity Manager instance or the load balancer.
Reverse Proxy	Deploy a reverse proxy such as F5 Access Policy Manager in the DMZ to allow users to securely access the VMware Identity Manager user portal remotely.

Port Requirements

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

- To sync users and groups from Active Directory, VMware Identity Manager must connect to Active Directory.
- To sync with ThinApp, the VMware Identity Manager must join the Active Directory domain and connect to the ThinApp Repository share.

Port	Portal	Source	Target	Description
443	HTTPS	Load Balancer	VMware Identity Manager virtual appliance	
443	HTTPS	VMware Identity Manager virtual appliance	VMware Identity Manager virtual appliance	
443	HTTPS	Browsers	VMware Identity Manager virtual appliance	
443	HTTPS	VMware Identity Manager virtual appliance	vapp-updates.vmware.com	Access to the upgrade server
8443	HTTPS	Browsers	VMware Identity Manager virtual appliance	Administrator Port
25	SMTP	VMware Identity Manager virtual appliance	SMTP	Port to relay outbound mail
389 636 3268 3269	LDAP LDAPS MSFT-GC MSFT-GC-SSL	VMware Identity Manager virtual appliance	Active Directory	Default values are shown. These ports are configurable.
445	TCP	VMware Identity Manager virtual appliance	VMware ThinApp repository	Access to the ThinApp repository

Port	Portal	Source	Target	Description
5500	UDP	VMware Identity Manager virtual appliance	RSA SecurID system	Default value is shown. This port is configurable.
53	TCP/UDP	VMware Identity Manager virtual appliance	DNS server	Every virtual appliance must have access to the DNS server on port 53 and allow incoming SSH traffic on port 22.
88, 464, 135	TCP/UDP	VMware Identity Manager virtual appliance	Domain controller	
9300–9400	TCP	VMware Identity Manager virtual appliance	VMware Identity Manager virtual appliance	Audit needs
54328	UDP			
1433, 5432, 1521	TCP	VMware Identity Manager virtual appliance	Database	Microsoft SQL default port is 1433 The Oracle default port is 1521
443		VMware Identity Manager virtual appliance	View server	Access to View server
80, 443	TCP	VMware Identity Manager virtual appliance	Citrix Integration Broker server	Connection to the Citrix Integration Broker. Port option depends on whether a certificate is installed on the Integration Broker server
443	HTTPS	VMware Identity Manager virtual appliance	AirWatch REST API	For device compliance checking and for the AirWatch Cloud Connector password authentication method, if that is used.
88	TCP/UDP	iOS mobile device	VMware Identity Manager virtual appliance	Port used for Kerberos traffic from iOS device to the built-in KDC.
5262	TCP	Android mobile device	AirWatch HTTPS proxy service	AirWatch Tunnel client routes traffic to the HTTPS proxy for Android devices.

Active Directory

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.

Supported Web Browsers to Access the Administration Console

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

- Internet Explorer 11 for Windows systems
- Google Chrome 42.0 or later for Windows and Mac systems
- Mozilla Firefox 40 or later for Windows and Mac systems
- Safari 6.2.8 and later for Mac systems

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

Supported Browsers to Access the 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.

Preparing to Deploy VMware Identity Manager

Before you deploy VMware Identity Manager, you must prepare your environment. This preparation includes downloading the VMware Identity Manager OVA file, creating DNS records, and obtaining IP addresses.

Prerequisites

Before you begin to install VMware Identity Manager complete the prerequisite tasks.

- You need one or more ESX servers to deploy the VMware Identity Manager virtual appliance.

  Note For information about supported vSphere and ESX server versions, see the VMware Product Interoperability Matrixes at http://www.vmware.com/resources/compatibility/sim/interop_matrix.php.

- VMware vSphere Client or vSphere Web Client is required to deploy the OVA file and access the deployed virtual appliance remotely to configure networking.
- Download the VMware Identity Manager OVA file from the VMware Web site.

Create DNS Records and IP Addresses

A DNS entry and a static IP address must be available for the VMware Identity Manager 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 1-1. 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 1-2. 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.

Using a Unix/Linux-based DNS Server

If you are using a Unix or Linux-based DNS server and plan to join VMware Identity Manager 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.

Database Options with VMware Identity Manager

Set up VMware Identity Manager with an external database to store and organize server data. An internal PostgreSQL database is embedded in the appliance but it is not recommended for use with production deployments.

To use an external database, your database administrator must prepare an empty external database and schema before connecting to the external database in the Setup wizard. Licensed users can use a Microsoft SQL database server or Oracle database server to set up a high availability external database environment. See "Connecting to the Database," on page 32.

Connecting to Your Enterprise Directory

VMware Identity Manager uses your enterprise directory infrastructure for user authentication and management. You can integrate VMware Identity Manager with an Active Directory environment that consists of a single Active Directory domain, multiple domains in a single Active Directory forest, or multiple domains across multiple Active Directory forests. You can also integrate VMware Identity Manager with an LDAP directory. To sync users and groups, the VMware Identity Manager virtual appliance must connect to the directory.

Your directory must be accessible in the same LAN network as the VMware Identity Manager virtual appliance.

See Chapter 4, "Integrating with Your Enterprise Directory," on page 43 for more information.

Deployment Checklists

You can use the deployment checklist to gather the necessary information to install the VMware Identity Manager virtual appliance.

Information for Fully Qualified Domain Name

Table 1-3. Fully Qualified Domain Name (FQDN) Information Checklist

Information to Gather	List the Information
VMware Identity Manager FQDN	

Network Information for VMware Identity Manager Virtual Appliance

Table 1-4. Network Information Checklist

Information to Gather	List the Information
IP address	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 1-5. 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 1-6. 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 VMware Identity Manager virtual appliance.

Table 1-7. SSL Certificate Information Checklist

Information to Gather	List the Information
SSL certificate	
Private key	

License Key

Table 1-8. VMware Identity Manager License Key Information Checklist

Information to Gather	List the Information
License key	

Note The License key information is entered in the administration console in the **Appliance Settings > License** page after the installation is complete.

External Database

Table 1-9. External Database Information Checklist

Information to Gather	List the Information
Database host name	
Port	
Username	
Password	

Customer Experience Improvement Program

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

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

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

Note If your network is configured to access the Internet through HTTP proxy, to send this information, you must adjust the proxy settings in the VMware Identity Manager virtual appliance. See "Setting Proxy Server Settings for VMware Identity Manager," on page 29.

Deploying VMware Identity Manager 2

To deploy VMware Identity Manager, you deploy the OVF template using the vSphere Client or the vSphere Web Client, power on the VMware Identity Manager virtual appliance, and configure settings.

After the VMware Identity Manager virtual appliance is deployed, you use the Setup wizard to set up the VMware Identity Manager environment.

Use the information in the deployment checklist to complete the installation. See "Deployment Checklists," on page 16.

This chapter includes the following topics:

Install the VMware Identity Manager OVA File

You deploy the VMware Identity Manager OVA file using the vSphere Client or the vSphere Web Client. You can download and deploy the OVA file from a local location that is accessible to the vSphere Client, or deploy it from a Web URL.

Note If you are using the vSphere Web Client, use either Firefox or Chrome browsers to deploy the OVA file. Do not use Internet Explorer.

Prerequisites

Review Chapter 1, "Preparing to Install VMware Identity Manager," on page 9.

Procedure

1 Download the VMware Identity Manager OVA file from My VMware.

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

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

4 In the Deploy OVF Template wizard, specify the following information.

Page	Description
Source	Browse to the OVA package location, or enter a specific URL.
OVF Template Details	Review the product details, including version and size requirements.
End User License Agreement	Read the End User License Agreement and click **Accept**.
Name and Location	Enter a name for the VMware Identity Manager virtual appliance. The name must be unique within the inventory folder and can contain up to 80 characters. Names are case sensitive. Select a location for the virtual appliance.
Host / Cluster	Select the host or cluster in which to run the virtual appliance.
Resource Pool	Select the resource pool.
Storage	Select the storage for the virtual appliance files. You can also select a VM Storage Profile.
Disk Format	Select the disk format for the files. For production environments, select one of the Thick Provision formats. Use the Thin Provision format for evaluation and testing. In the Thick Provision format, all the space required for the virtual disk is allocated during deployment. In the Thin Provision format, the disk uses only the amount of storage space that it needs for its initial operations.
Network Mapping	Map the networks used in VMware Identity Manager to networks in your inventory.
Properties	a In the **Timezone setting** field, select the correct time zone. b The **Customer Experience Improvement Program** checkbox is selected by default. VMware collects anonymous data about your deployment in order to improve VMware's response to user requirements. Deselect the checkbox if you do not want the data collected. c In the **Host Name (FQDN)** text box, enter the host name to use. If this is blank, reverse DNS is used to look up the host name. d Configure the networking properties. ■ To configure a static IP address for VMware Identity Manager, enter the address for the **Default Gateway**, **DNS**, **IP Address**, and **Netmask** fields. **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. **Important** If any of the four address fields, including **Host Name**, are left blank, DHCP is used. ■ To configure DHCP, leave the address fields blank. **Note** The **Domain Name** and **Domain Search Path** fields are not used. You can leave these blank. (Optional) After VMware Identity Manager is installed, you can configure IP Pools. See "(Optional) Add IP Pools," on page 21.
Ready to Complete	Review your selections and click **Finish**.

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

5 When the deployment is complete, click **Close** in the progress dialog box.

6 Select the VMware Identity Manager virtual appliance you deployed, right-click, and select **Power > Power on**.

The VMware Identity Manager virtual appliance is initialized. You can go to the **Console** tab to see the details. When the virtual appliance initialization is complete, the console screen displays the VMware Identity Manager version, IP address, and the URLs to log in to the VMware Identity Manager Web interface and to complete the set up.

What to do next

- (Optional) Add IP Pools.
- Configure VMware Identity Manager settings, including connecting to your Active Directory or LDAP directory and selecting users and groups to sync to VMware Identity Manager.

(Optional) Add IP Pools

Network configuration with IP Pools is optional in VMware Identity Manager. You can manually add IP pools to the VMware Identity Manager virtual appliance after it is installed.

IP Pools act like DHCP servers to assign IP addresses from the pool to the VMware Identity Manager virtual appliance. To use IP Pools, you edit the virtual appliance networking properties to change the properties to dynamic properties and configure the netmask, gateway, and DNS settings.

Prerequisites

The virtual appliance must be powered off.

Procedure

1. In the vSphere Client or the vSphere Web Client, right-click the VMware Identity Manager virtual appliance and select **Edit Settings**.
2. Select the **Options** tab.
3. Under **vApp Options**, click **Advanced**.
4. In the Properties section on the right, click the **Properties** button.
5. In the Advanced Property Configuration dialog box, configure the following keys:
   - vami.DNS.WorkspacePortal
   - vami.netmask0.WorkspacePortal
   - vami.gateway.WorkspacePortal

   a. Select one of the keys and click **Edit**.

   b. In the Edit Property Settings dialog box, next to the **Type** field, click **Edit**.

   c. In the Edit Property Type dialog box, select **Dynamic Property** and select the appropriate value from the drop down menu for **Netmask**, **Gateway Address**, and **DNS Servers** respectively.

   d. Click **OK**, and click **OK** again.

   e. Repeat these steps to configure each key.
6. Power on the virtual appliance.

The properties are configured to use IP Pools.

What to do next

Configure VMware Identity Manager settings.

Configure VMware Identity Manager Settings

After the VMware Identity Manager OVA is deployed, you use the Setup wizard to set passwords and select a database. Then you set up the connection to your Active Directory or LDAP directory.

Prerequisites

- The VMware Identity Manager virtual appliance is powered on.

- If you are using an external database, the external database is configured and the external database connection information is available. See "Connecting to the Database," on page 32 for information.
- Review Chapter 4, "Integrating with Your Enterprise Directory," on page 43, "Integrating with Active Directory," on page 44, and "Integrate an LDAP Directory with the Service," on page 58 for requirements and limitations.
- You have your Active Directory or LDAP directory information.
- When multi-forest Active Directory is configured and the Domain Local group contains members from domains in different forests, the Bind DN user used on the VMware Identity Manager Directory page must be added to the Administrators group of the domain in which Domain Local group resides. If this is not done, these members will be missing from the Domain Local group.
- You have a list of the user attributes you want to use as filters, and a list of the groups you want to add to VMware Identity Manager.

Procedure

1 Go to the VMware Identity Manager URL that is shown on the blue screen in the **Console** tab. For example, `https://hostname.example.com`.

2 Accept the certificate, if prompted.

3 In the Get Started page, click **Continue**.

4 In the Set Passwords page, set passwords for the following administrator accounts, which are used to manage the appliance, then click **Continue**.

Account	
Appliance Administrator	Set the password for the **admin** user. This user name cannot be changed. The **admin** user account is used to manage the appliance settings. **IMPORTANT** The **admin** user password must be at least 6 characters in length.
Appliance Root	Set the **root** user password. The **root** user has full rights to the appliance.
Remote User	Set the **sshuser** password, which is used to log in remotely to the appliance with an SSH connection.

5 In the Select Database page, select the database to use.

See "Connecting to the Database," on page 32 for more information.

- If you are using an external database, select **External Database** and enter the external database connection information, user name, and password. To verify that VMware Identity Manager can connect to the database, click **Test Connection**.

  After you verify the connection, click **Continue**.
- If you are using the internal database, click **Continue**.

  NOTE The internal database is not recommended for use with production deployments.

The connection to the database is configured and the database is initialized. When the process is complete, the **Setup is complete** page appears.

6 Click the **Log in to the administration console** link on the **Setup is complete** page to log in to the administration console to set up the Active Directory or LDAP directory connection.

7 Log in to the administration console as the **admin** user, using the password you set.

You are logged in as a Local Admin. The Directories page appears. Before you add a directory, ensure that you review Chapter 4, "Integrating with Your Enterprise Directory," on page 43, "Integrating with Active Directory," on page 44, and "Integrate an LDAP Directory with the Service," on page 58 for requirements and limitations.

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

9 Click **Setup > User Attributes** to select the user attributes to sync to the directory.

Default attributes are listed and you can select the ones that are required. If an attribute is marked required, only users with that attribute are synced to the service. You can also add other attributes.

Important After a directory is created, you cannot change an attribute to be a required attribute. You must make that selection now.

Also, be aware that the settings in the User Attributes page apply to all directories in the service. When you mark an attribute required, consider the effect on other directories. If an attribute is marked required, users without that attribute are not synced to the service.

Important If you plan to sync XenApp resources to VMware Identity Manager, you must make **distinguishedName** a required attribute.

---

10 Click **Save**.

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

12 In the Directories page, click **Add Directory** and select **Add Active Directory over LDAP/IWA** or **Add LDAP Directory**, based on the type of directory you are integrating.

You can also create a local directory in the service. For more information about using local directories, see Chapter 5, "Using Local Directories," on page 63.

13 For Active Directory, follow these steps.

a Enter a name for the directory you are creating in VMware Identity Manager and select the type of directory, either **Active Directory over LDAP** or **Active Directory (Integrated Windows Authentication)**.

b Provide the connection information.

Option	Description
Active Directory over LDAP	1 In the **Sync Connector** field, select the connector you want to use to sync users and groups from Active Directory to the VMware Identity Manager directory. A connector component is always available with the VMware Identity Manager service by default. This connector appears in the drop-down list. If you install multiple VMware Identity Manager appliances for high availability, the connector component of each appears in the list. 2 In the **Authentication** field, select **Yes** if you want to use this Active Directory to authenticate users. If you want to use a third-party identity provider 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. 3 In the **Directory Search Attribute** field, select the account attribute that contains username. 4 If the Active Directory uses DNS Service Location lookup, make the following selections. ■ In the **Server Location** section, select the **This Directory supports DNS Service Location** checkbox. A `domain_krb.properties` file, auto-populated with a list of domain controllers, will be created when the directory is created. See "About Domain Controller Selection (domain_krb.properties file)," on page 47 . ■ 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. 5 If the Active Directory does not use DNS Service Location lookup, make the following selections. ■ In the **Server Location** section, verify that the **This Directory supports DNS Service Location** checkbox is not selected and enter the Active Directory server host name and port number. To configure the directory as a global catalog, see the Multi-Domain, Single Forest Active Directory Environment section in "Active Directory Environments," on page 45. ■ If the Active Directory requires access over SSL, select the **This Directory requires all connections to use SSL** check box in the **Certificates** section and copy and paste the Active Directory Root CA certificate into the **SSL Certificate** field. Ensure the certificate is in PEM format and include the "BEGIN CERTIFICATE" and "END CERTIFICATE" lines. **Note** If the Active Directory requires SSL and you do not provide the certificate, you cannot create the directory.

Option	Description
	6 In the **Allow Change Password** section, select **Enable Change Password** if you want to allow users to reset their passwords from the VMware Identity Manager login page if the password expires or if the Active Directory administrator resets the user's password. 7 In the **Base DN** field, enter the DN from which to start account searches. For example, OU=myUnit,DC=myCorp,DC=com. 8 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. 9 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)	1 In the **Sync Connector** field, select the connector you want to use to sync users and groups from Active Directory to the VMware Identity Manager directory. A connector component is always available with the VMware Identity Manager service by default. This connector appears in the drop-down list. If you install multiple VMware Identity Manager appliances for high availability, the connector component of each appears in the list. 2 In the **Authentication** field, if you want to use this Active Directory to authenticate users, click **Yes**. If you want to use a third-party identity provider 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. 3 In the **Directory Search Attribute** field, select the account attribute that contains username. 4 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. 5 Enter the name of the Active Directory domain to join. Enter a user name and password that has the rights to join the domain. See "Permissions Required for Joining a Domain," on page 52 for more information. 6 In the **Allow Change Password** section, select **Enable Change Password** if you want to allow users to reset their passwords from the VMware Identity Manager login page if the password expires or if the Active Directory administrator resets the user's password. 7 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. 8 Enter the Bind DN User password.

c Click **Save & Next**.

The page with the list of domains appears.

14 For LDAP directories, follow these steps.

a Provide the connection information.

Option	Description
Directory Name	A name for the directory you are creating in VMware Identity Manager.
Directory Sync and Authentication	1 In the **Sync Connector** field, select the connector you want to use to sync users and groups from your LDAP directory to the VMware Identity Manager directory. A connector component is always available with the VMware Identity Manager service by default. This connector appears in the drop-down list. If you install multiple VMware Identity Manager appliances for high availability, the connector component of each appears in the list. You do not need a separate connector for an LDAP directory. A connector can support multiple directories, regardless of whether they are Active Directory or LDAP directories. 2 In the **Authentication** field, select **Yes** if you want to use this LDAP directory to authenticate users. 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. 3 In the **Directory Search Attribute** field, specify the LDAP directory attribute to be used for user name. If the attribute is not listed, select **Custom** and type the attribute name. For example, **`cn`**.
Server Location	Enter the LDAP Directory server host and port number. For the server host, you can specify either the fully-qualified domain name or the IP address. For example, **`myLDAPserver.example.com`** or **`100.00.00.0`**. If you have a cluster of servers behind a load balancer, enter the load balancer information instead.
LDAP Configuration	Specify the LDAP search filters and attributes that VMware Identity Manager can use to query your LDAP directory. Default values are provided based on the core LDAP schema. **LDAP Queries** ■ **Get groups**: The search filter for obtaining group objects. For example: **`(objectClass=group)`** ■ **Get bind user**: The search filter for obtaining the bind user object, that is, the user that can bind to the directory. For example: **`(objectClass=person)`** ■ **Get user**: The search filter for obtaining users to sync. For example: **`(&(objectClass=user)(objectCategory=person))`** **Attributes** ■ **Membership**: The attribute that is used in your LDAP directory to define the members of a group. For example: **`member`** ■ **Object UUID**: The attribute that is used in your LDAP directory to define the UUID of a user or group. For example: **`entryUUID`** ■ **Distinguished Name**: The attribute that is used in your LDAP directory for the distinguished name of a user or group. For example: **`entryDN`**

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

b 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.

c Click **Save & Next**.

The page listing the domain appears.

15 For an LDAP directory, the domain is listed and cannot be modified.

For Active Directory over LDAP, the domains are listed and cannot be modified.

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**.

16 Verify that the VMware Identity Manager attribute names are mapped to the correct Active Directory or LDAP attributes and make changes, if necessary.

Important If you are integrating an LDAP directory, you must specify a mapping for the **domain** attribute.

17 Click **Next**.

18 Select the groups you want to sync from your Active Directory or LDAP directory to the VMware Identity Manager directory.

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** If you have multiple groups with the same name in your LDAP directory, you must specify unique names for them in VMware Identity Manager. You can change the name while selecting the group. **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. 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.

19 Click **Next**.

20 Specify additional users to sync, if required.

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.

21 Click **Next**.

22 Review the page to see how many users and groups will sync 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.

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

Note If a networking error occurs and the host name cannot be uniquely resolved using reverse DNS, the configuration process stops. You must fix the networking problems and restart the virtual appliance. Then, you can continue the deployment process. The new network settings are not available until after you restart the virtual appliance.

What to do next

For information about setting up a load balancer or a high-availability configuration, see Chapter 6, "Advanced Configuration for the VMware Identity Manager Appliance," on page 71.

You can customize the catalog of resources for your organization's applications and enable user access to these resources. You can also set up other resources, including View, ThinApp, and Citrix-based applications. See *Setting up Resources in VMware Identity Manager*.

Setting Proxy Server Settings for VMware Identity Manager

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

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

Note Proxy servers that require authentication are not supported.

Procedure

1. From the vSphere Client, log in as the root user to the VMware Identity Manager virtual appliance.
2. Enter `YaST` on the command line to run the `YaST` utility.
3. Select **Network Services** in the left pane, then select **Proxy**.
4. Enter the proxy server URLs in the **HTTP Proxy URL** and **HTTPS Proxy URL** fields.
5. Select **Finish** and exit the `YaST` utility.
6. Restart the Tomcat server on the VMware Identity Manager virtual appliance to use the new proxy settings.

   ```
   service horizon-workspace restart
   ```

The cloud application catalog and other Web services are now available in VMware Identity Manager.

Enter the License Key

After you deploy the VMware Identity Manager appliance, enter your license key.

Procedure

1. Log in to the VMware Identity Manager administration console.
2. Select the **Appliance Settings** tab, then click **License**.
3. In the License Settings page, enter the license key and click **Save**.

Managing Appliance System Configuration Settings

3

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

You can also update the database, FQDN, and syslog, and download log files.

Page Name	Setting Description
Database Connection	The database connection setting, either Internal or External, is enabled. You can change the database type. When you select External Database, you enter the external database URL, user name, and password. To set up an external database, see "Connecting to the Database," on page 32.
Install Certificate	On this page, you install a custom or self-signed certificate for VMware Identity Manager and, if VMware Identity Manager is configured with a load balancer, you can install the load balancer's root certificate. The location of the VMware Identity Manager root CA certificate is displayed on this page as well, on the **Terminate SSL on a Load Balancer** tab. See "Using SSL Certificates," on page 35.
Identity Manager FQDN	The VMware Identity Manager FQDN is displayed on this page. You can change it. VMware Identity Manager FQDN is the URL that users use to access the service.
Configure Syslog	On this page, you can enable an external syslog server. VMware Identity Manager logs are sent to this external server. See "Enable the Syslog Server," on page 39.
Change Password	On this page, you can change the VMware Identity Manager admin user password.
System Security	On this page, you can change the root password for the VMware Identity Manager appliance and the ssh user password used to log in remotely.
Log File Locations	A list of log files and their directory locations is displayed on this page. You can bundle the log files into a zip file to download. See "Log File Information," on page 39.

You can also modify the connector URL. See "Modifying the Connector URL," on page 38.

This chapter includes the following topics:

Change Appliance Configuration Settings

After you configure VMware Identity Manager, you can go to the Appliance Settings pages to update the current configuration and monitor system information for the virtual appliance.

Procedure

1 Log in to the administration console.

2 Select the **Appliance Settings** tab and click **Manage Configuration**.

3 Log in with the service administrator password.

4 In the left pane, select the page to view or edit.

What to do next

Verify that the settings or updates you make are in effect.

Connecting to the Database

An internal PostgreSQL database is embedded in the VMware Identity Manager appliance but it is not recommended for use with production deployments. To use an external database with VMware Identity Manager, your database administrator must prepare an empty database and schema before connecting to the database in VMware Identity Manager.

You can connect to the external database connection when you run the VMware Identity Manager Setup wizard. You can also go to the Appliance Settings > VA Configuration > Database Connection Setup page to configure the connection to the external database.

Licensed users can use an external Oracle database or Microsoft SQL Server to set up a high availability database environment.

Configure a Microsoft SQL Database

To use a Microsoft SQL database for the VMware Identity Manager, you must create a new database in the Microsoft SQL server.

You create for a database named **saas** on the Microsoft SQL server and create a login user named **horizon**.

Note The default collation is case-sensitve.

Prerequisites

- Supported version of the Microsoft SQL server installed as an external database server.
- Load balancing implementation configured.
- Administrator rights to access and create the database components using Microsoft SQL Server Management Studio or from another Microsoft SQL Server CLI client.

Procedure

1 Log in to the Microsoft SQL Server Management Studio session as the sysadmin or a user account with sysadmin privileges.

The editor window appears.

2 In the toolbar, click **New Query**.

3 Cut and paste the following commands into the editor window.

Microsoft SQL Commands

```
CREATE DATABASE saas
COLLATE Latin1_General_CS_AS;
ALTER DATABASE saas SET READ_COMMITTED_SNAPSHOT ON;
GO
BEGIN
CREATE LOGIN horizon WITH PASSWORD = N'H0rizon!';
END
GO
USE saas;
IF EXISTS (SELECT * FROM sys.database_principals WHERE name = N'horizon')
DROP USER [horizon]
GO
CREATE USER horizon FOR LOGIN horizon
WITH DEFAULT_SCHEMA = saas;
GO
CREATE SCHEMA saas AUTHORIZATION horizon
GRANT ALL ON DATABASE::saas TO horizon;
GO
```

4 On the toolbar, click **!Execute**.

The Microsoft SQL database server is now ready to be connected to the VMware Identity Manager database

What to do next

Configure the external database on the VMware Identity Manager server. Go to the VMware Identity Manager administration console Appliance Settings > VA Configuration > Database Connection Setup page. Enter the JDBC URL as **`jdbc:sqlserver://<hostname-or-DB_VM_IP_ADDR>;DatabaseName=saas`**. Enter the user name and password created for the database. See "Configure VMware Identity Manager to Use an External Database," on page 35

Configure an Oracle Database

During the Oracle database installation, you must specify certain Oracle configurations for optimum performance with VMware Identity Manager.

Prerequisites

The Oracle database you create is going to be called `saas`. VMware Identity Manager requires Oracle quoted identifiers for the username and schema. Therefore, you must use double quotes when you create the Oracle `saas` username and schema.

Procedure

1 Specify the following settings when creating an Oracle database.

   a Select the **General Purpose/Transaction Processing Database** configuration option.

   b Click **Use Unicode > UTF8**.

   c Use National Character Set.

2 Connect to the Oracle database after the installation is finished.

3 Log in to the Oracle database as the sys user.

4 Increase the process connections. Each additional service virtual machine requires a minimum of 300 process connections to function with VMware Identity Manager. For example, if your environment has two service virtual machines, run the `alter` command as sys or system user.

   a Increase the process connections using the `alter` command.

   ```
   alter system set processes=600 scope=spfile
   ```

   b Restart the database.

5 Create a database trigger that all users can use.

Sample SQL to Create a Database Trigger

```
CREATE OR REPLACE
TRIGGER CASE_INSENSITIVE_ONLOGON
AFTER LOGON ON DATABASE
DECLARE
username VARCHAR2(30);
BEGIN
username:=SYS_CONTEXT('USERENV','SESSION_USER');
IF username = 'saas' THEN
execute immediate 'alter session set NLS_SORT=BINARY_CI';
execute immediate 'alter session set NLS_COMP=LINGUISTIC';
END IF;
EXCEPTION
WHEN OTHERS THEN
NULL;
END;
```

6 Run the Oracle commands to create a new user schema.

Sample SQL to Create a New User

```
CREATE USER "saas"
IDENTIFIED BY <password>
DEFAULT TABLESPACE USERS
TEMPORARY TABLESPACE TEMP
PROFILE DEFAULT
ACCOUNT UNLOCK;
GRANT RESOURCE TO "saas" ;
GRANT CONNECT TO "saas" ;
ALTER USER "saas" DEFAULT ROLE ALL;
GRANT UNLIMITED TABLESPACE TO "saas";
```

Administering the Internal Database

The internal PostgreSQL database is configured and ready to use by default. Note that the internal database is not recommended for use with production deployments.

When the VMware Identity Manager is installed and powered on, during the initialization process, a random password for the internal database user is generated. This password is unique to each deployment and can be found in the file `/usr/local/horizon/conf/db.pwd`.

To configure your internal database for high availability, see KB 2094258.

Configure VMware Identity Manager to Use an External Database

After you set up the database in the VMware Identity Manager Setup wizard, you can configure VMware Identity Manager to use a different database.

You must point VMware Identity Manager to an initialized, populated database. For example, you can use a database configured as the result of a successful run of the VMware Identity Manager Setup wizard, a database from a backup, or an existing database from a recovered snapshot.

Prerequisites

- Install and configure the supported Microsoft SQL or Oracle edition as the external database server. For information about specific versions that are supported by VMware Identity Manager, see the VMware Product Interoperability Matrixes at http://www.vmware.com/resources/compatibility/sim/interop_matrix.php.

Procedure

1 In the administration console click **Appliance Settings** and select **VA Configuration**.

2 Click **Manage Configuration**.

3 Log in with the VMware Identity Manager administrator password.

4 On the Database Connection Setup page, select **External Database** as the database type.

5 Enter information about the database connection.

   a Type the JDBC URL of the database server.

Microsoft SQL	`jdbc:sqlserver://hostname_or_IP_address;DatabaseName=horizon`
Oracle	`jdbc:oracle:thin:@//hostname_or_IP_address:port/sid`

   b Type the name of the user with read and write privileges to the database.

Microsoft SQL	`horizon`
Oracle	“saas”

   c Type the password for the user you created when you configured the database.

6 Click **Test Connection** to verify and save the information.

Using SSL Certificates

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

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

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

You can install a signed CA certificate from the **Appliance Settings > Manage Configuration > Install Certificate** page. You can also add the load balancer's root CA certificate on this page as well.

Apply Public Certificate Authority

When the VMware Identity Manager service is installed, a default SSL server certificate is generated. You can use the default certificate for testing purposes. You should generate and install commercial SSL certificates for your environment.

Note If the VMware Identity Manager points to a load balancer, the SSL certificate is applied to the load balancer.

Prerequisites

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

Procedure

1 In the administration console, click **Appliance Settings**.

VA configuration is selected by default.

2 Click **Manage Configuration**.

3 In the dialog box that appears, enter the VMware Identity Manager server admin user password.

4 Select **Install Certificate**.

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

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

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

Ensure that the certificate includes the FQDN hostname.

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

8 Click **Save.**

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-----

Adding SSL Certificates

When you apply the certificate make sure that you include the entire certificate chain. The certificate to be installed must be in the PEM format.

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

Important You must add the certificate chain in the order of SSL Certificate, Intermediate CA Certificates, Root CA Certificate.

Certificate Chain Example
-----BEGIN CERTIFICATE-----
SSL Cert - Appliance SSL Cert
-----END CERTIFICATE-----

Certificate Chain Example
-----BEGIN CERTIFICATE-----
Intermediate/Issuing CA Cert
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
Root CA Cert
-----END CERTIFICATE-----

Modifying the VMware Identity Manager Service URL

You can change the VMware Identity Manager service URL, which is the URL that users use to access the service. For example, you might change the URL to a load balancer URL.

Procedure

1 Log into the VMware Identity Manager administration console.

2 Click the **Appliance Settings** tab, then select **VA Configuration**.

3 Click **Manage Configuration** and log in with the **`admin`** user password.

4 Click **Identity Manager FQDN** and enter the new URL in the **Identity Manager FQDN** field.

Use the format **`https://`*`FQDN`*`:`*`port`**. Specifying a port is optional. The default port is 443.

For example, **`https://myservice.example.com`**.

5 Click **Save**.

What to do next

Enable the new portal user interface.

1 Go to https://*VMwareIdentityManagerURL*/admin to access the administration console.

2 In the administration console, click the arrow on the **Catalog** tab and select **Settings**.

3 Select **New End User Portal UI** in the left pane and click **Enable New Portal UI**.

Modifying the Connector URL

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

Procedure

1 Log in to the VMware Identity Manager administration console.

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

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

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

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

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

5 Click **Save**.

Enable the Syslog Server

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

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

If you do not specify a syslog server during the initial configuration, you can configure it later from the **Appliance Settings > VA Configuration > Manage Configuration > Syslog Configuration** page.

Prerequisites

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

Procedure

1 Log in to the administration console.

2 Click the **Appliance Settings** tab, select **VA Configuration** in the left pane, and click **Manage Configuration**.

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

4 Click **Enable**.

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

6 Click **Save.**

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

Log File Information

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

Table 3-1. Log Files

Component	Location of Log File	Description
Identity Manager Service Logs	`/opt/vmware/horizon/workspace/logs/horizon.log`	Information about activity on the VMware Identity Manager application, such as entitlements, users, and groups.
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.

Table 3-1. Log Files (Continued)

Component	Location of Log File	Description
Update Logs	`/opt/vmware/var/log/update.log` `/opt/vmware/var/log/vami`	A record of output messages related to update requests during an upgrade of VMware Identity Manager. The files in the `/opt/vmware/var/log/vami` directory are useful for troubleshooting. You can find these files on all virtual machines after an upgrade.
Apache Tomcat Logs	`/opt/vmware/horizon/workspace/logs/catalina.log`	Apache Tomcat records of messages that are not recorded in other log files.

Collect Log Information

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

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

Procedure

1 Log in to the administration console.

2 Select the **Appliance Settings** tab and click **Manage Configuration**.

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

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

4 Download the prepared bundle.

What to do next

To collect all logs, do this on each appliance.

Manage Your Appliance Passwords

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

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

Procedure

1 In the administration console, click the **Appliance Settings** tab.

2 Click **VA Configuration > Manage Configuration**.

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

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

4 Enter the new password.

5 Click **Save**.

Configure SMTP Settings

Configure SMTP server settings to receive email notifications from the VMware Identity Manager service.

Notification emails are sent to new users that are created as local users and when a password is reset in the VMware Identity Manager service.

Procedure

1 Log in to the administration console.

2 Select the **Appliance Settings** tab and click **SMTP**.

3 Enter the SMTP server host name.

For example: `smtp.example.com`

4 Enter the SMTP server port number.

For example: `25`

5 (Optional) Enter a user name and password, if the SMTP server requires authentication.

6 Click **Save**.

Integrating with Your Enterprise Directory

4

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

The following types of directories are supported.

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

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

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

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

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.

Connector

The connector, a component of the service, performs the following functions.

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

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

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

Directory

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

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

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

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

Worker

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

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

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

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," on page 43.

Active Directory Environments

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

Single Active Directory Domain Environment

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

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

For more information, see:

- "About Domain Controller Selection (domain_krb.properties file)," on page 47
- "Managing User Attributes that Sync from Active Directory," on page 50
- "Permissions Required for Joining a Domain," on page 52
- "Configuring Active Directory Connection to the Service," on page 52

Multi-Domain, Single Forest Active Directory Environment

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

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

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

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

  For more information, see:

  - "About Domain Controller Selection (domain_krb.properties file)," on page 47
  - "Managing User Attributes that Sync from Active Directory," on page 50
  - "Permissions Required for Joining a Domain," on page 52
  - "Configuring Active Directory Connection to the Service," on page 52
- If Integrated Windows Authentication does not work in your Active Directory environment, create an Active Directory over LDAP directory type and select the global catalog option.

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

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

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

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

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

Multi-Forest Active Directory Environment with Trust Relationships

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

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

For more information, see:

- "About Domain Controller Selection (domain_krb.properties file)," on page 47
- "Managing User Attributes that Sync from Active Directory," on page 50
- "Permissions Required for Joining a Domain," on page 52
- "Configuring Active Directory Connection to the Service," on page 52

Multi-Forest Active Directory Environment Without Trust Relationships

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

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

For more information, see:

- "About Domain Controller Selection (domain_krb.properties file)," on page 47
- "Managing User Attributes that Sync from Active Directory," on page 50
- "Permissions Required for Joining a Domain," on page 52
- "Configuring Active Directory Connection to the Service," on page 52

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` file is created in the virtual machine that contains the connector. In a typical deployment, with no additional connectors deployed, the file is created in the VMware Identity Manager service virtual machine. If you are using an additional connector for the directory, the file is created in the connector virtual machine. A virtual machine can only have one `domain_krb.properties` file.
- The file is created, and auto-populated with domain controllers for each domain, when you first create a directory that has DNS Service Location lookup enabled.
- Domain controllers for each domain are listed in order of priority. To connect to Active Directory, the connector tries the first domain controller in the list. If it is not reachable, it tries the second one in the list, and so on.
- The file is updated only when you create a new directory that has DNS Service Location lookup enabled or when you add a domain to an Integrated Windows Authentication directory. The new domain and a list of domain controllers for it are added to the file.

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

For information on editing the `domain_krb.properties` file, see "Editing the domain_krb.properties file," on page 49.

Important The `/etc/krb5.conf` file must be consistent with the `domain_krb.properties` file. Whenever you update the `domain_krb.properties` file, also update the `krb5.conf` file. See "Editing the domain_krb.properties file," on page 49 and Knowledge Base article 2091744 for more information.

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

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

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

- The subnet of the connector must be present in the Active Directory configuration, or a subnet must be specified in the `runtime-config.properties` file. See "Overriding the Default Subnet Selection," on page 48.

  The subnet is used to determine the site.

- The Active Directory configuration must be site aware.

If the subnet cannot be determined or if your Active Directory configuration is not site aware, DNS Service Location lookup is used to find domain controllers, and the file is populated with a few domain controllers that are reachable. Note that these domain controllers may not be at the same geographical location as the connector, which can result in delays or timeouts while communicating with Active Directory. In this case, edit the `domain_krb.properties` file manually and specify the correct domain controllers to use for each domain. See "Editing the domain_krb.properties file," on page 49.

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 VMware Identity Manager virtual machine as the root user.

  Note If you are using an additional connector for the directory, log in to the connector virtual machine.

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

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

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

  `siteaware.subnet.override=10.100.0.0/20`

3 Save and close the file.

4 Restart the service.

```
service horizon-workspace restart
```

Editing the domain_krb.properties file

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

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

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

See also "About Domain Controller Selection (domain_krb.properties file)," on page 47.

Procedure

1 Log in to the VMware Identity Manager virtual machine as the root user.

Note If you are using an additional connector for the directory, log in to the connector virtual machine.

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

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

Use the following format:

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

For example:

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

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

Important Domain names must be in lowercase.

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

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

5 Restart the service.

```
service horizon-workspace restart
```

What to do next

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

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

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

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

2 Restart the workspace service.

```
service horizon-workspace restart
```

See also Knowledge Base article 2091744.

Troubleshooting domain_krb.properties

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

"Error resolving domain" error

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

Domain controllers are unreachable

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

Managing User Attributes that Sync from Active Directory

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

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

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

Table 4-1. Default Active Directory Attributes to Sync to Directory

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

Select Attributes to Sync with Directory

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

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

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

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

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

Procedure

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

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

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

4 Click **Save**.

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

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

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

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

8 Click **Save.**

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

Permissions Required for Joining a Domain

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

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

- Create Computer Objects
- Delete Computer Objects

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

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

- Select which attributes are required and add additional attributes, if necessary, on the User Attributes page. See "Select Attributes to Sync with Directory," on page 51.

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

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

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

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

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

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

Procedure

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

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

3 Enter a name for this VMware Identity Manager directory.

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

Option	Description
Active Directory over LDAP	a In the **Sync Connector** field, select the connector to use to sync with Active Directory. b In the **Authentication** field, if this Active Directory is used to authenticate users, click **Yes**. If a third-party identity provider is used to authenticate users, click **No**. After you configure the Active Directory connection to sync users and groups, go to the Identity & Access Management > Manage > Identity Providers page to add the third-party identity provider for authentication. c In the **Directory Search Attribute** field, select the account attribute that contains username. d If the Active Directory uses DNS Service Location lookup, make the following selections. ■ In the **Server Location** section, select the **This Directory supports DNS Service Location** checkbox. A `domain_krb.properties` file, auto-populated with a list of domain controllers, will be created when the directory is created. See "About Domain Controller Selection (domain_krb.properties file)," on page 47 . ■ If the Active Directory requires STARTTLS encryption, select the **This Directory requires all connections to use SSL** check box in the **Certificates** section and copy and paste the Active Directory Root CA certificate into the **SSL Certificate** field. Ensure the certificate is in PEM format and include the "BEGIN CERTIFICATE" and "END CERTIFICATE" lines. **Note** If the Active Directory requires STARTTLS and you do not provide the certificate, you cannot create the directory. e If the Active Directory does not use DNS Service Location lookup, make the following selections. ■ In the **Server Location** section, verify that the **This Directory supports DNS Service Location** checkbox is not selected and enter the Active Directory server host name and port number. To configure the directory as a global catalog, see the Multi-Domain, Single Forest Active Directory Environment section in "Active Directory Environments," on page 45. ■ If the Active Directory requires access over SSL, select the **This Directory requires all connections to use SSL** check box in the **Certificates** section and copy and paste the Active Directory Root CA certificate into the **SSL Certificate** field. Ensure the certificate is in PEM format and include the "BEGIN CERTIFICATE" and "END CERTIFICATE" lines. **Note** If the Active Directory requires SSL and you do not provide the certificate, you cannot create the directory. f In the **Base DN** field, enter the DN from which to start account searches. For example, OU=myUnit,DC=myCorp,DC=com. g In the **Bind DN** field, enter the account that can search for users. For example, CN=binduser,OU=myUnit,DC=myCorp,DC=com. **Note** Using a Bind DN user account with a non-expiring password is recommended. h After you enter the Bind password, click **Test Connection** to verify that the directory can connect to your Active Directory.
Active Directory (Integrated Windows Authentication)	a In the **Sync Connector** field, select the connector to use to sync with Active Directory . b In the **Authentication** field, if this Active Directory is used to authenticate users, click **Yes**.

Option	Description
	If a third-party identity provider is used to authenticate users, click **No**. After you configure the Active Directory connection to sync users and groups, go to the Identity & Access Management > Manage > Identity Providers page to add the third-party identity provider for authentication.
	c In the **Directory Search Attribute** field, select the account attribute that contains username.
	d If the Active Directory requires STARTTLS encryption, select the **This Directory requires all connections to use STARTTLS** checkbox in the **Certificates** section and copy and paste the Active Directory Root CA certificate into the **SSL Certificate** field. Ensure the certificate is in PEM format and include the "BEGIN CERTIFICATE" and "END CERTIFICATE" lines. If the directory has multiple domains, add the Root CA certificates for all domains, one at a time. **Note** If the Active Directory requires STARTTLS and you do not provide the certificate, you cannot create the directory.
	e Enter the name of the Active Directory domain to join. Enter a user name and password that has the rights to join the domain. See "Permissions Required for Joining a Domain," on page 52 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.

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. 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.

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

What to do next

- If you created a directory that supports DNS Service Location, a `domain_krb.properties` file was created and auto-populated with a list of domain controllers. View the file to verify or edit the list of domain controllers. See "About Domain Controller Selection (domain_krb.properties file)," on page 47.

- Set up authentication methods. After users and groups sync to the directory, if the connector is also used for authentication, you can set up additional authentication methods on the connector. If a third party is the authentication identity provider, configure that identity provider in the connector.
- Review the default access policy. The default access policy is configured to allow all appliances in all network ranges to access the Web browser, 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 when you add Web applications to the catalog, you can create new ones.
- Apply custom branding to the administration console, user portal pages and the sign-in screen.

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.

- If you use additional, standalone connector virtual appliances, note that the **Allow Change Password** option is only available with connector version 2016.11.1 and 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.

Prerequisites

- Port 464 must be open from VMware Identity Manager to the domain controllers.

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," on page 43.

Limitations of LDAP Directory Integration

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

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

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

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

Integrate an LDAP Directory with the Service

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

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

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

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

Specifically, you need to provide the following information.

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

Certain limitations apply to the LDAP directory integration feature. See "Limitations of LDAP Directory Integration," on page 58.

Prerequisites

- If you use additional, external connector virtual appliances, note that the ability to integrate LDAP directories is only available with connector version 2016.6.1 and later.
- Review the attributes in the **Identity & Access Management > Setup > User Attributes** page and add additional attributes that you want to sync. You map these VMware Identity Manager attributes to your LDAP directory attributes later when you create the directory. These attributes are synced for the users in the directory.

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

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

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

Procedure

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

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

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

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

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

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

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

5 Click **Save & Next**.

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

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

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

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

8 Click **Next**.

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

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

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

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

10 Click **Next**.

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

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

Click **Next**.

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

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

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

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

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 the connector component of each of the service instances to the new directory.

Procedure

1 Log in to the VMware Identity Manager administration console.

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

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

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

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

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

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

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

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

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

Using Local Directories 5

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.

The local administrator user that is created when you first set up the VMware Identity Manager appliance is created in the System Domain of the System Directory.

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.

1 Set User Attributes at the Global Level on page 65

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

2 Create a Local Directory on page 66

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

3 Associate the Local Directory With an Identity Provider on page 68

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.

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 5-1. 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
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.

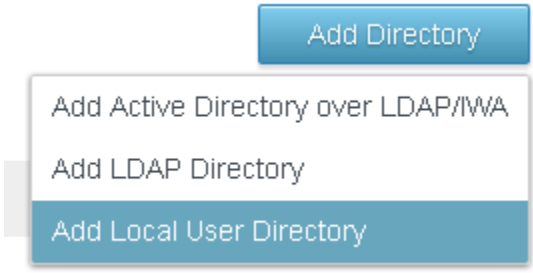
Create a Local Directory

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

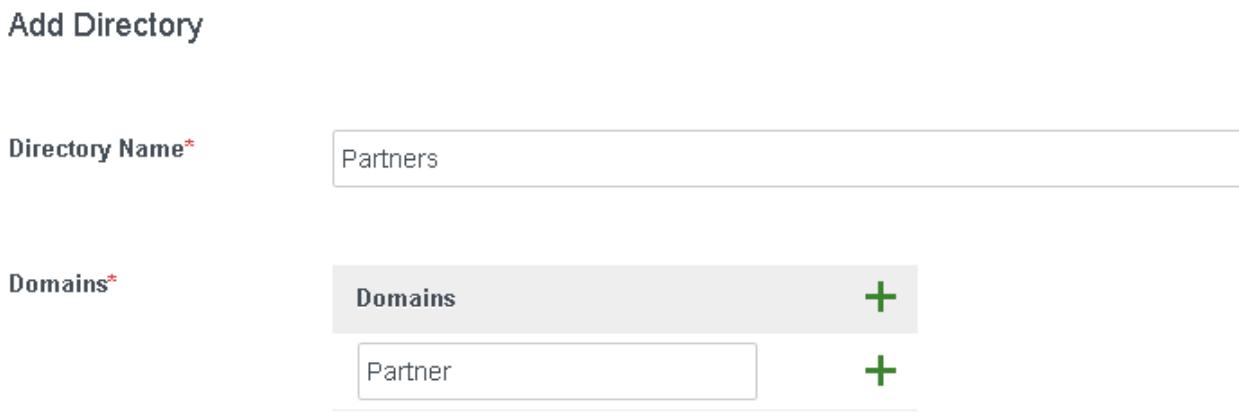
2 Click **Add Directory** and select **Add Local User Directory** from the drop-down menu.



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.

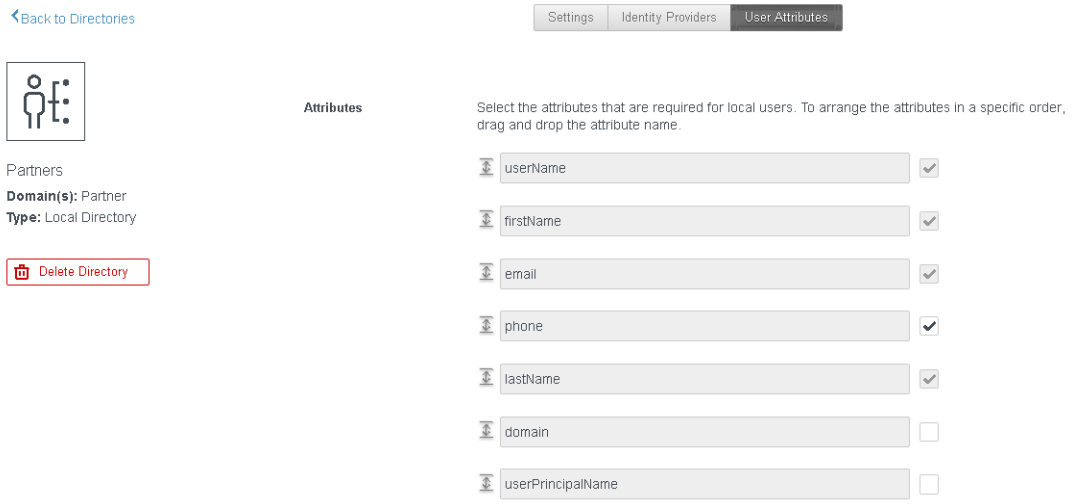
You can specify which attributes are required and which attributes are optional. You can also change the order in which the attributes appear.

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.

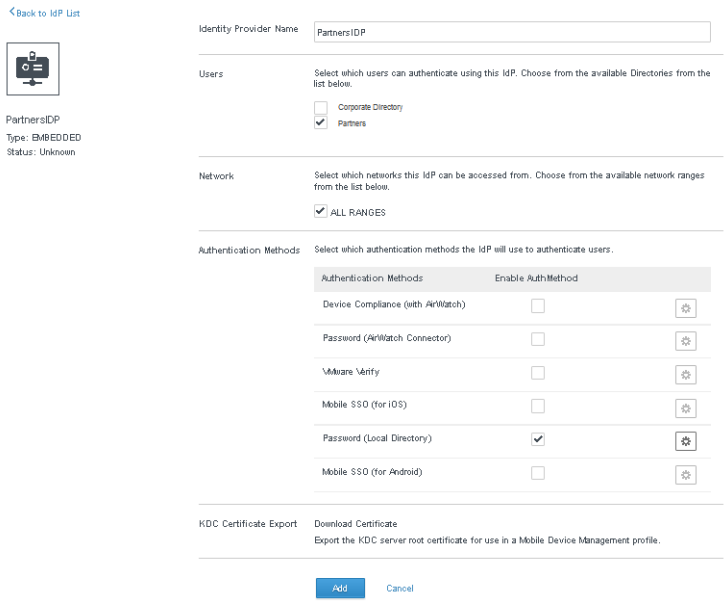
Procedure

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.
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**.

Advanced Configuration for the VMware Identity Manager Appliance 6

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

The VMware Identity Manager architecture diagram demonstrates how you can deploy the VMware Identity Manager environment. See Chapter 1, "Preparing to Install VMware Identity Manager," on page 9 for a typical deployment.

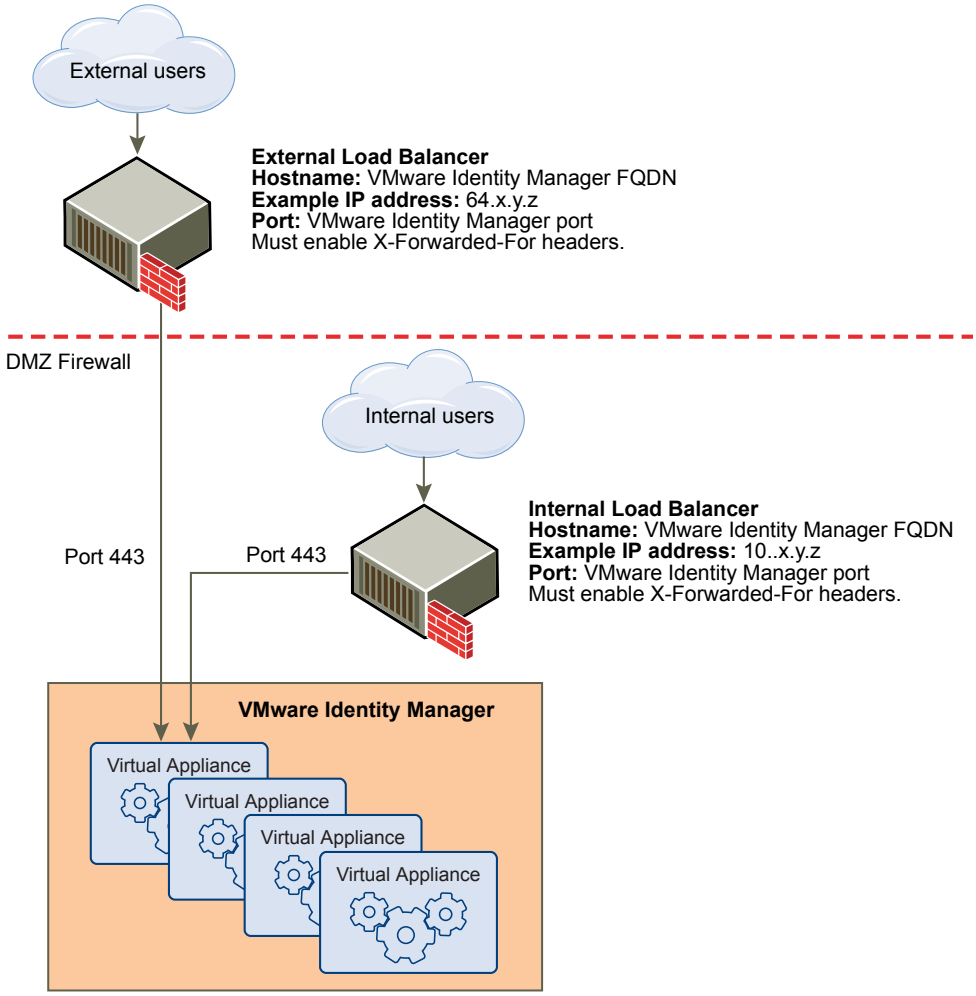
This chapter includes the following topics:

Using a Load Balancer or Reverse Proxy to Enable External Access to VMware Identity Manager

During deployment, the VMware Identity Manager virtual appliance is set up inside the internal network. If you want to provide access to the service for users connecting from outside networks, you must install a load balancer or a reverse proxy, such as Apache, nginx, or F5, in the DMZ.

If you do not use a load balancer or reverse proxy, you cannot expand the number of VMware Identity Manager appliances later. You might need to add more appliances to provide redundancy and load balancing. The following diagram shows the basic deployment architecture you can use to enable external access.

Figure 6-1. External Load Balancer Proxy with Virtual Machine



Specify VMware Identity Manager FQDN during Deployment

During the deployment of the VMware Identity Manager virtual machine, you enter the VMware Identity Manager FQDN and port number. These values must point to the host name that you want end users to access.

The VMware Identity Manager virtual machine always runs on port 443. You can use a different port number for the load balancer. If you use a different port number, you must specify it during deployment.

Load Balancer Settings to Configure

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

- X-Forwarded-For Headers

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

- Load Balancer Timeout

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

- Enable Sticky Sessions

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

Apply VMware Identity Manager Root Certificate to the Load Balancer

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

The VMware Identity Manager certificate can be downloaded from the administration console, from the **Appliance Settings > VA Configuration > Manage Configuration** page.

If the VMware Identity Manager FQDN points to a load balancer, the SSL certificate can only be applied to the load balancer.

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

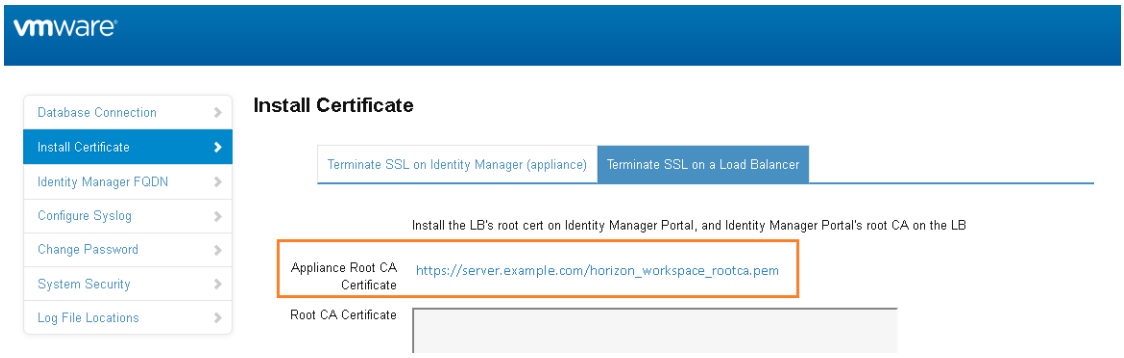
Procedure

1 In the administration console, select the **Appliance Settings** tab and select **VA Configuration**.

2 Click **Manage Configuration**.

3 Select **Install Certificate**.

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



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

What to do next

Copy and paste the load balancer root certificate to the VMware Identity Managerconnector appliance.

Apply Load Balancer Root Certificate to VMware Identity Manager

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

Procedure

1 Obtain the load balancer root certificate.

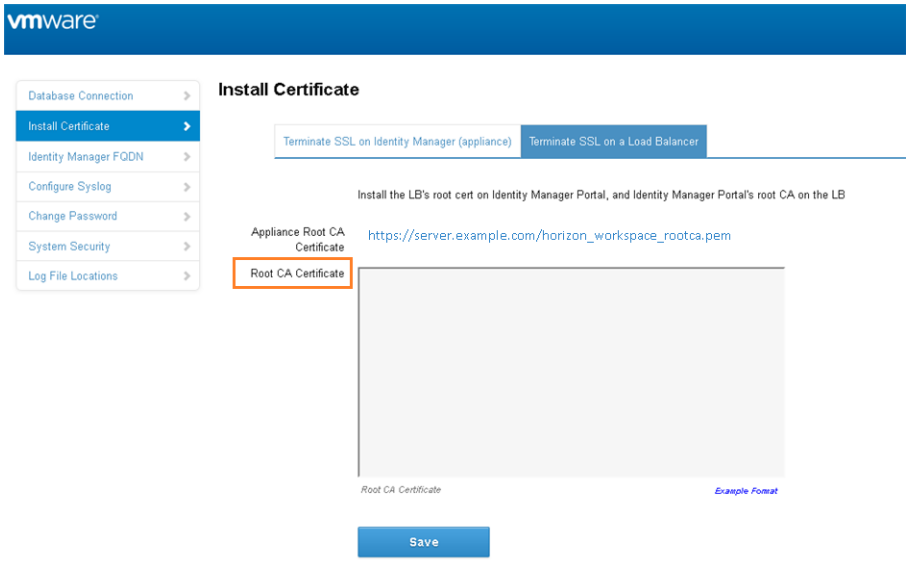
2 In the VMware Identity Manager administration console, select the **Appliance Settings** tab and select **VA Configuration**.

3 Click **Manage Configuration**.

4 Log in with the admin user password.

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

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



7 Click **Save**.

Setting Proxy Server Settings for VMware Identity Manager

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

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

Note Proxy servers that require authentication are not supported.

Procedure

1 From the vSphere Client, log in as the root user to the VMware Identity Manager virtual appliance.

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

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

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

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

6 Restart the Tomcat server on the VMware Identity Manager virtual appliance to use the new proxy settings.

```
service horizon-workspace restart
```

The cloud application catalog and other Web services are now available in VMware Identity Manager.

Configuring Failover and Redundancy in a Single Datacenter

To achieve failover and redundancy, you can add multiple VMware Identity Manager virtual appliances in a cluster. If one of the virtual appliances shuts down for any reason, VMware Identity Manager is still available.

You first install and configure a VMware Identity Manager virtual appliance, then you clone it. Cloning the virtual appliance creates a duplicate of the appliance with the same configuration as the original. You can customize the cloned virtual appliance to change the name, network settings, and other properties as required.

Before you clone the VMware Identity Manager virtual appliance, you must configure it behind a load balancer and change its Fully Qualified Domain Name (FQDN) to match the load balancer FQDN. Also, complete directory configuration in the VMware Identity Manager service before you clone the appliance.

After cloning, you assign the cloned virtual appliance a new IP address before powering it on. The cloned virtual appliance IP address must follow the same guidelines as the IP address of the original virtual appliance. The IP address must resolve to a valid host name using forward and reverse DNS.

All nodes in the VMware Identity Manager cluster are identical and nearly stateless copies of each other. Syncing to Active Directory and to resources that are configured, such as View or ThinApp, is disabled on the cloned virtual appliances.

1 Recommended Number of Nodes in VMware Identity Manager Cluster on page 75

   Setting up a VMware Identity Manager cluster with three nodes is recommended.

2 Change VMware Identity Manager FQDN to Load Balancer FQDN on page 76

   Before you clone the VMware Identity Manager virtual appliance, you must change its Fully Qualified Domain Name (FQDN) to match the load balancer FQDN.

3 Clone the Virtual Appliance on page 77

4 Assign a New IP Address to Cloned Virtual Appliance on page 78

   You must assign a new IP address to each cloned virtual appliance before you power it on. The IP address must be resolvable in DNS. If the address is not in the reverse DNS, you must also assign the host name.

5 Enabling Directory Sync on Another Instance in the Event of a Failure on page 79

Recommended Number of Nodes in VMware Identity Manager Cluster

Setting up a VMware Identity Manager cluster with three nodes is recommended.

The VMware Identity Manager appliance includes Elasticsearch, a search and analytics engine. Elasticsearch has a known limitation with clusters of two nodes. For a description of the Elasticsearch "split brain" limitation, see the Elasticsearch documentation. Note that you do not have to configure any Elasticsearch settings.

A VMware Identity Manager cluster with two nodes provides failover capability with a few limitations related to Elasticsearch. If one of the nodes shuts down, the following limitations apply until the node is brought up again:

- The dashboard does not display data.
- Most reports are unavailable.
- Sync log information is not displayed for directories.
- The search field in the top-right corner of the administration console does not return any results.
- Auto-complete is not available for text fields.

There is no data loss during the time the node is down. Audit event and sync log data is stored and will be displayed when the node is restored.

Change VMware Identity Manager FQDN to Load Balancer FQDN

Before you clone the VMware Identity Manager virtual appliance, you must change its Fully Qualified Domain Name (FQDN) to match the load balancer FQDN.

Prerequisites

- The VMware Identity Manager appliance is added to a load balancer.
- You have applied the load balancer root CA certificate to VMware Identity Manager.

Procedure

1 Log in to the VMware Identity Manager administration console.

2 Select the **Appliance Settings** tab.

3 In the Virtual Appliance Configuration page, click **Manage Configuration**.

4 Enter your administrator password to log in.

5 Click **Identity Manager Configuration**.

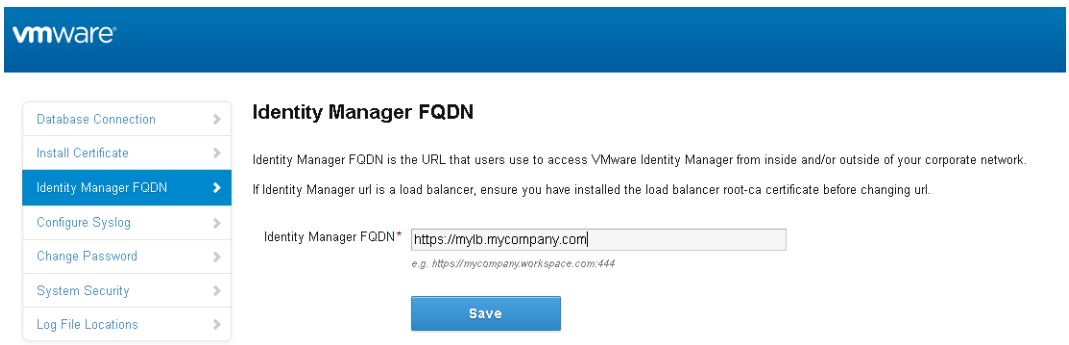
6 In the **Identity Manager FQDN** field, change the host name part of the URL from the VMware Identity Manager host name to the load balancer host name.

For example, if your VMware Identity Manager host name is `myservice` and your load balancer host name is `mylb`, you would change the URL

`https://myservice.mycompany.com`

to the following:

`https://mylb.mycompany.com`



7 Click **Save**.

- The service FQDN is changed to the load balancer FQDN.
- The Identity Provider URL is changed to the load balancer URL.

What to do next

Clone the virtual appliance.

Clone the Virtual Appliance

Clone the VMware Identity Manager virtual appliance to create multiple virtual appliances of the same type to distribute traffic and eliminate potential downtime.

Using multiple VMware Identity Manager virtual appliances improves availability, load balances requests to the service, and decreases response times to the end user.

Prerequisites

- The VMware Identity Manager virtual appliance must be 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 and is unique to each virtual appliance.
- An external database is configured as described in "Connecting to the Database," on page 32.
- Ensure that you complete directory configuration in VMware Identity Manager.
- Log in to the virtual appliance console as root and delete the `/etc/udev/rules.d/70-persistent-net.rules` file, if it exists. If you do not delete this file before cloning, networking is not configured correctly on the cloned virtual appliance.

Procedure

1. Log in to the vSphere Client or vSphere Web Client and navigate to the VMware Identity Manager virtual appliance.
2. Right-click the virtual appliance and select **Clone**.
3. Enter the name for the cloned virtual appliance and click **Next**.

   The name must be unique within the VM folder.
4. Select the host or cluster on which to run the cloned virtual appliance and click **Next**.
5. Select the resource pool in which to run the virtual appliance and click **Next**.
6. For the virtual disk format, select **Same format as source**.
7. Select the data store location where you want to store the virtual appliance files and click **Next**.
8. Select **Do not customize** as the guest operating system option.
9. Review the options and click **Finish**.

The cloned virtual appliance is deployed. You cannot use or edit the virtual appliance until the cloning is complete.

What to do next

Assign an IP address to the cloned virtual appliance before you power it on and add it to the load balancer.

Assign a New IP Address to Cloned Virtual Appliance

You must assign a new IP address to each cloned virtual appliance before you power it on. The IP address must be resolvable in DNS. If the address is not in the reverse DNS, you must also assign the host name.

Procedure

1 In the vSphere Client or the vSphere Web Client, select the cloned virtual appliance.

2 In the **Summary** tab, under **Commands**, click **Edit Settings**.

3 Select **Options** and in the **vApp Options** list, select **Properties**.

4 Change the IP address in the **IP Address** field.

5 If the IP address is not in the reverse DNS, add the host name in the **HostName** text box.

6 Click **OK.**

7 Power on the cloned appliance and wait until the blue login screen appears in the **Console** tab.

Important Before you power on the cloned appliance, ensure that the original appliance is fully powered on.

What to do next

- Wait for a few minutes until the Elasticsearch and RabbitMQ clusters are created before adding the cloned virtual appliance to the load balancer.

  Elasticsearch, a search and analytics engine, and RabbitMQ, a messaging broker, are embedded in the virtual appliance.

  a Log in to the cloned virtual appliance.

  b Check the Elasticsearch cluster:

  ```
  curl –XGET 'http://localhost:9200/_cluster/health?pretty=true'
  ```

  Verify that the result matches the number of nodes.

  c Check the RabbitMQ cluster:

  ```
  rabbitmqctl cluster_status
  ```

  Verify that the result matches the number of nodes.

- Add the cloned virtual appliance to the load balancer and configure the load balancer to distribute traffic. See your load balancer vendor documentation for information.

- If you had joined a domain in the original service instance, then you need to join the domain in the cloned service instances.

  a Log in to the VMware Identity Manager administration console.

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

  The connector component of each of the cloned service instances is listed in the Connectors page.

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

  For more information about Active Directory, see "Integrating with Active Directory," on page 44.

- For directories of type Integrated Windows Authentication (IWA), you must do the following:

  a For the cloned service instances, join the domain to which the IWA directory in the original service instance was joined.

  1 Log in to the VMware Identity Manager administration console.

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

The connector component of each of the cloned service instances is listed in the Connectors page.

3 For each connector listed, 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.

- If you had manually updated the `/etc/krb5.conf` file in the original service instance, for example, to resolve View synchronization failure or slowness, you must update the file in the cloned instance after the cloned instance is joined to the domain. In all the cloned service instances, perform the following tasks.

  a 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.

  b Restart the workspace service.

```
service horizon-workspace restart
```

  Note Also see Knowledge Base article 2091744.

- Enable the authentication methods configured for connector on each of the cloned instances. See the *VMware Identity Manager Administration Guide* for information.

The VMware Identity Manager service virtual appliance is now highly available. Traffic is distributed to the virtual appliances in your cluster based on the load balancer configuration. Authentication to the service is highly available. For the directory sync feature of the service, however, in the event of a service instance failure, you will need to manually enable directory sync on a cloned service instance. Directory sync is handled by the connector component of the service and can only be enabled on one connector at a time. See "Enabling Directory Sync on Another Instance in the Event of a Failure," on page 79.

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

In the event of a service instance failure, authentication is handled automatically by a cloned instance, as configured in the load balancer. However, for directory sync, you need to modify the directory settings in the VMware Identity Manager service to use a cloned instance. Directory sync is handled by the connector component of the service and can only be enabled on one connector at a time.

Procedure

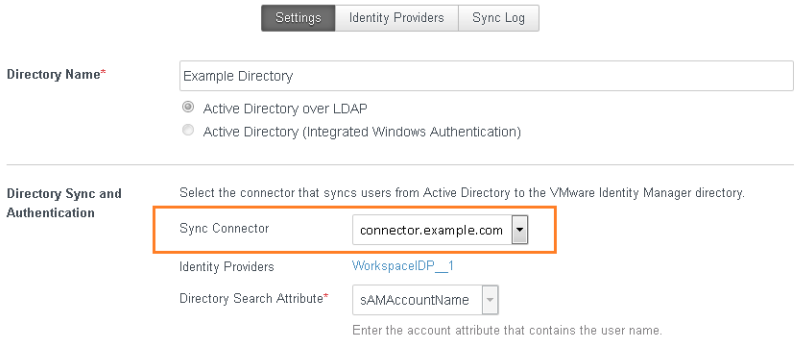
1 Log in to the VMware Identity Manager administration console.

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

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

You can view this information in the **Setup > Connectors** page. The page lists the connector component of each of the service virtual appliances in your cluster.

4 In the **Directory Sync and Authentication** section of the directory page, in the **Sync Connector** field, select one of the other connectors.



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

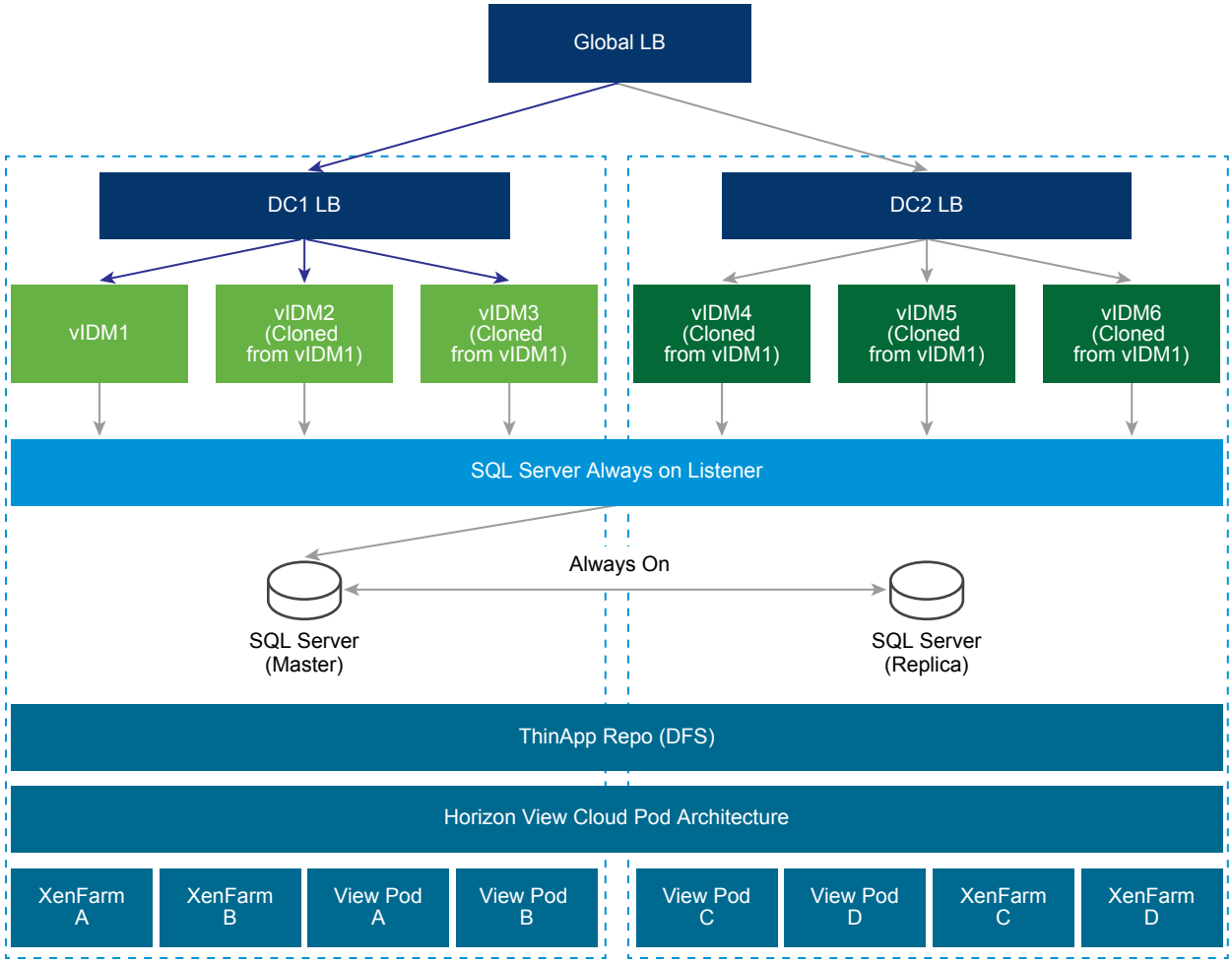
6 Click **Save**.

Deploying VMware Identity Manager in a Secondary Data Center for Failover and Redundancy

To provide failover capabilities if the primary VMware Identity Manager data center becomes unavailable, VMware Identity Manager needs to be deployed in a secondary data center.

By using a secondary data center, end users can log in and use applications with no downtime. A secondary data center also allows administrators the ability to upgrade VMware Identity Manager to the next version without any downtime. See "Upgrading VMware Identity Manager with No Downtime," on page 91.

A typical deployment using a secondary data center is shown here.



Follow these guidelines for a multi-data center deployment.

- Cluster Deployment: You need to deploy a set of three or more VMware Identity Manager virtual appliances as one cluster in one data center and another set of three or more virtual appliances as another cluster in the second data center. See "Setting up a Secondary Data Center," on page 82 for more information.
- Database: VMware Identity Manager uses the database to store data. For a multi-datacenter deployment, replication of the database between the two data centers is crucial. Refer to your database documentation about how to set up a database in multiple data centers. For example, with SQL Server, using Always On deployment is recommended. See Overview of Always On Availability Groups (SQL Server) on the Microsoft website for information. VMware Identity Manager functionalities expect very low latency between the database and the VMware Identity Manager appliance. Therefore, appliances in one data center are expected to connect to the database in the same data center.
- Not Active-Active: VMware Identity Manager does not support an Active-Active deployment where users can be served from both data centers at the same time. The secondary data center is a hot stand-by and can be used to provide business continuity for end users. VMware Identity Manager appliances in the secondary data center are in a read-only mode. Therefore, after a fail-over to that data center, most admin operations, like adding users or apps, or entitling users, will not work.
- Fail-Back to Primary: In most failure scenarios, you can fail back to the primary data center once that data center is back to normal. See "Failback to Primary Data Center," on page 91 for information.

- Promote Secondary to Primary: In case of an extended data center failure, the secondary data center can be promoted to primary. See "Promoting Secondary Data Center to Primary Data Center," on page 91 for information.
- Fully Qualified Domain Name: The fully qualified domain name to access VMware Identity Manager should be the same in all data centers.
- Audits: VMware Identity Manager uses Elasticsearch embedded in the VMware Identity Manager appliance for auditing, reports, and directory sync logs. Separate Elasticsearch clusters have to be created in each data center. See "Setting up a Secondary Data Center," on page 82 for more information.
- Active Directory: VMware Identity Manager can connect to Active Directory using the LDAP API or using Integrated Windows Authentication. In both these methods, VMware Identity Manager can leverage Active Directory SRV records to reach the appropriate domain controller in each data center.
- Windows Apps: VMware Identity Manager supports accessing Windows apps using ThinApp, and Windows Apps and Desktops using Horizon View or Citrix technologies. It is usually important to deliver these resources from a data center that is closer to the user, also called Geo-Affinity. Note the following about Windows resources:
  - ThinApps - VMware Identity Manager supports Windows Distributed File Systems as a ThinApp repository. Use the Windows Distributed File Systems documentation to set up appropriate location-specific policies.
  - Horizon View (with Cloud Pod Architecture) - VMware Identity Manager supports Horizon Cloud Pod Architecture. Horizon Cloud Pod Architecture provides Geo-Affinity using global entitlements. See "Integrating Cloud Pod Architecture Deployments" in *Setting up Resources in VMware Identity Manager* for information. No additional changes are required for a VMware Identity Manager multi-datacenter deployment.
  - Horizon View (without Cloud Pod Architecture) - If Horizon Cloud Pod Architecture is not enabled in your environment, you cannot enable Geo-Affinity. After a fail-over event, you can manually switch VMware Identity Manager to launch Horizon View resources from the View pods configured in the secondary data center. See "Configure Failover Order of Horizon View and Citrix-based Resources," on page 87 for more information.
  - Citrix Resources - Similar to Horizon View (without Cloud Pod Architecture), you cannot enable Geo-Affinity for Citrix resources. After a fail-over event, you can manually switch VMware Identity Manager to launch Citrix resources from the XenFarms configured in the secondary data center. See "Configure Failover Order of Horizon View and Citrix-based Resources," on page 87 for more information.

Setting up a Secondary Data Center

The secondary data center is typically managed by a different vCenter Server. When you set up the secondary data center, you can configure and implement the following based on your requirements.

- VMware Identity Manager appliances in the secondary data center, created from an OVA file imported from the primary data center
- Load balancer for the secondary data center
- Duplicate Horizon View and Citrix-based resources and entitlements
- Database configuration
- Load balancer or DNS entry across the primary and secondary data centers for failover

Modify the Primary Data Center for Replication

Before you set up the secondary data center, configure the primary data center for Elasticsearch, RabbitMQ, and Ehcache replication across clusters.

Elasticsearch, RabbitMQ, and Ehcache are embedded in the VMware Identity Manager virtual appliance. Elasticsearch is a search and analytics engine used for auditing, reports, and directory sync logs. RabbitMQ is a messaging broker. Ehcache provides caching capabilities.

Configure these changes in all the nodes in the primary data center cluster.

Prerequisites

You have set up a VMware Identity Manager cluster in the primary data center.

Procedure

1 Configure Elasticsearch for replication.

  Make these changes in each node of the primary data center cluster.

  a Disable the cron job for Elasticsearch.

    1 Edit the `/etc/cron.d/hznelasticsearchsync` file:

      ```
      vi /etc/cron.d/hznelasticsearchsync
      ```

    2 Comment out this line:

      ```
      #*/1 * * * * root /usr/local/horizon/scripts/elasticsearchnodes.hzn
      ```

  b Add the IP addresses of all the nodes in the primary data center cluster.

    1 Edit the `/etc/sysconfig/elasticsearch` file.

      ```
      vi /etc/sysconfig/elasticsearch
      ```

    2 Add the IP addresses of all the nodes in the cluster:

      ```
      ES_UNICAST_HOSTS=IPaddress1,IPaddress2,IPaddress3
      ```

  c Add the load balancer FQDN of the secondary data center cluster to the `/usr/local/horizon/conf/runtime-config.properties` file.

    1 Edit the `/usr/local/horizon/conf/runtime-config.properties` file.

      ```
      vi /usr/local/horizon/conf/runtime-config.properties
      ```

    2 Add this line to the file:

      ```
      analytics.replication.peers=LB_FQDN_of_second_cluster
      ```

2 Configure RabbitMQ for replication.

Make these changes in each node of the primary data center cluster.

a Disable the cron job for RabbitMQ.

1 `vi /etc/cron.d/hznrabbitmqsync`

2 Comment out this line:

```
#*/1 * * * * root /usr/local/horizon/scripts/rabbitmqnodes.hzn
```

b Make the following changes in the `/usr/local/horizon/scripts/rabbitmqnodes.hzn` file.

1 `vi /usr/local/horizon/scripts/rabbitmqnodes.hzn`

2 Comment out these lines.

```
#make sure SAAS is up, otherwise we won't have an accurate node list
#if test $(curl –X GET –k https://localhost/SAAS/API/1.0/REST/system/health/allOk –
sL –w "% {http_code}\\n" –o /dev/null) –ne 200 ; then
#    echo SAAS not running, aborting
#    exit 0
#fi
```

Also comment out the following line.

```
#nodes=$(uniqList true $(enumeratenodenames))
```

3 Add the host names of all the nodes in the primary data center cluster. Use the host names only, not the fully qualified domain names. Separate the names with a space.

```
nodes="node1 node2 node3"
```

c Add the IP address and host name mapping of the other nodes in the cluster to the `/etc/hosts` file. Do not add an entry for the node you are editing. This step is only required if there is no DNS entry that can resolve the fully-qualified domain name or partially-qualified domain names.

```
IPaddress node2FQDN node2

IPaddress node3FQDN node3
```

d Run the script to build the RabbitMQ cluster.

```
/usr/local/horizon/scripts/rabbitmqnodes.hzn
```

3 Configure Ehcache for replication.

Make these changes in each node of the primary data center cluster.

a `vi /usr/local/horizon/conf/runtime–config.properties`

b Add the FQDN of the other nodes in the cluster. Do not add the FQDN of the node you are editing. Separate FQDNs by a colon.

```
ehcache.replication.rmi.servers=node2FQDN:node3FQDN
```

For example:

```
ehcache.replication.rmi.servers=server2.example.com:server3.example.com
```

4 Restart the VMware Identity Manager service on all nodes.

```
service horizon–workspace restart
```

5 Verify that the cluster is set up correctly.

Run these commands on all the nodes in the first cluster.

a Verify the health of Elasticsearch.

```
curl 'http://localhost:9200/_cluster/health?pretty'
```

The command should return a result similar to the following.

```
        {
  "cluster_name" : "horizon",
  "status" : "green",
  "timed_out" : false,
  "number_of_nodes" : 3,
  "number_of_data_nodes" : 3,
  "active_primary_shards" : 20,
  "active_shards" : 40,
  "relocating_shards" : 0,
  "initializing_shards" : 0,
  "unassigned_shards" : 0,
  "delayed_unassigned_shards" : 0,
  "number_of_pending_tasks" : 0,
  "number_of_in_flight_fetch" : 0
}
```

If there are problems, see "Troubleshooting Elasticsearch and RabbitMQ," on page 102.

b Verify the health of RabbitMQ.

```
rabbitmqctl cluster_status
```

The command should return a result similar to the following.

```
Cluster status of node 'rabbitmq@node3' ...
[{nodes,[{disc,['rabbitmq@node2','rabbitmq@node3']}]},
 {running_nodes,['rabbitmq@node3']},
 {cluster_name,<<"rabbitmq@node2.example.com">>},
 {partitions,[]},
 {alarms,[{'rabbitmq@node3',[]}]}]
```

If there are problems, see "Troubleshooting Elasticsearch and RabbitMQ," on page 102.

c Verify that the `/opt/vmware/horizon/workspace/logs/ horizon.log` file contains this line.

```
Added ehcache replication peer: //node3.example.com:40002
```

The host names should be those of the other nodes in the cluster.

What to do next

Create a cluster in the secondary data center. Create the nodes by exporting the OVA file of the first VMware Identity Manager virtual appliance from the primary data center cluster and using it to deploy the new virtual appliances in the secondary data center..

Create VMware Identity Manager Virtual Appliances in Secondary Data Center

To set up a VMware Identity Manager cluster in the secondary data center, you export the OVA file of the original VMware Identity Manager appliance in the primary data center and use it to deploy appliances in the secondary data center.

Prerequisites

- VMware Identity Manager OVA file that was exported from the original VMware Identity Manager appliance in the primary data center
- IP addresses and DNS records for secondary data center

Procedure

1 In the primary data center, export the OVA file of the original VMware Identity Manager appliance.

See the vSphere documentation for information.

2 In the secondary data center, deploy the VMware Identity Manager OVA file that was exported to create the new nodes.

See the vSphere documentation for information. Also see "Install the VMware Identity Manager OVA File," on page 19.

3 After the VMware Identity Manager appliances are powered on, update the appliance configuration for each.

The VMware Identity Manager appliances in the secondary data center are identical copies of the original VMware Identity Manager appliance in the primary data center. Syncing to Active Directory and to resources that are configured in the primary data center is disabled.

What to do next

Go to the administration console pages and configure the following:

- Enable Join Domain as configured in the original VMware Identity Manager appliance in the primary data center.
- In the Auth Adapters page, add the authentication methods that are configured in the primary data center.
- In the Directory Authentication Method page, enable Windows Authentication, if configured in the primary data center.

Go to the appliance settings Install Certificate page to add Certificate Authority signed certificates, duplicating the certificates in the VMware Identity Manager appliances in the primary data center. See "Using SSL Certificates," on page 35.

Configure Nodes in Secondary Data Center

After you create nodes in the secondary data center by using the OVA file exported from the primary data center, configure the nodes.

Follow these steps for each node in the secondary data center.

Procedure

- Update IP tables.
  a. Verify that the `/usr/local/horizon/conf/flags/enable.rabbitmq` file exists.

     ```
     touch /usr/local/horizon/conf/flags/enable.rabbitmq
     ```

  b. In the `/usr/local/horizon/scripts/updateiptables.hzn` file, update the IP addresses of all nodes in the secondary data center.

     1. `vi /usr/local/horizon/scripts/updateiptables.hzn`
     2. Find and replace the `ALL_IPS` line. Specify the IP addresses delimited by a space.

        ```
        ALL_IPS="Node1_IPaddress Node2_IPaddress Node3_IPaddress"
        ```

     3. Open ports by running this script.

        ```
        /usr/local/horizon/scripts/updateiptables.hzn
        ```

  c. Configure the nodes for Elasticsearch, RabbitMQ, and Ehcache replication and verify that they are set up correctly.

     See the instructions in "Modify the Primary Data Center for Replication," on page 83 and apply them to the nodes in the secondary data center.

     Note that the cron jobs are already disabled.

Edit runtime-config.properties File in Secondary Data Center

If you are using a database other than a SQL Server Always On deployment, you must edit the `runtime-config.properties` files for the VMware Identity Manager appliances in the secondary data center to change the JDBC URL to point to the database in the secondary data center and to configure the appliance for read-only access. If you are using a SQL Server Always On deployment, this step is not required.

Make these changes in each VMware Identity Manager appliance in the secondary data center.

Procedure

1. Using a ssh client, log in to the VMware Identity Manager appliance as the root user.
2. Open the `runtime-config.properties` file at `/usr/local/horizon/conf/runtime-config.properties`.
3. Change the JDBC URL to point to the database for the secondary data center.

   See "Configure VMware Identity Manager to Use an External Database," on page 35.
4. Configure the VMware Identity Manager appliance to have read-only access.

   Add the line `read.only.service=true`.
5. Restart the Tomcat server on the appliance.

   ```
   service horizon-workspace restart
   ```

Configure Failover Order of Horizon View and Citrix-based Resources

For Horizon View and Citrix-based resources, you must configure the failover order of resources in both the primary and secondary data centers to make the appropriate resources available from any data center.

You use the hznAdminTool command to create a database table with the failover order for resources in your organization per service instance. The configured failover order is followed when a resource is launched. You run the `hznAdminTool failoverConfiguration` in both data centers to set up the failover order.

Prerequisites

When VMware Identity Manager is deployed in multiple data centers, the same resources are also set up in each data center. Each application or desktop pool in the View Pods or Citrix-based XenFarms is considered as a different resource in the VMware Identity Manager catalog. To prevent duplication of the resource in the catalog, make sure that you enabled **Do not sync duplicate applications** in the View Pools or Published Apps - Citrix pages in the administration console page.

Procedure

1 Using a ssh client, log in to the VMware Identity Manager appliance as the root user.

2 To view a list of the server instances, type `hznAdminTool serviceInstances`.

A list of the service instances with the ID number assigned displays, as in this example.

```
{"id":103,"hostName":"ws4.domain.com","ipaddress":"10.142.28.92"}{"id":
154,"hostName":"ws3.domain.com","ipaddress":"10.142.28.91"}{"id":
1,"hostName":"ws1.domain.com","ipaddress":"10.143.104.176"}{"id":
52,"hostName":"ws2.domain.com","ipaddress":"10.143.104.177"}
```

3 For each service instance in your organization, configure the failover order for View and Citrix-based resources.

Type `hznAdminTool failoverConfiguration –configType <configType> –configuration <configuration> –serviceInstanceId <serviceInstanceId> [–orgId <orgId>]`

Option	Description
-configType	Type the resource type being configured for failover. Values are either `VIEW` or `XENAPP`.
-configuration	Type the failover order. For VIEW configType, type as a comma separated list of the primary View Connector Server host names that are listed in the View Pools page in the administration console. For XENAPP configType, type as a comma separated list of XenFarm names.
-serviceInstanceId	Type the ID of the service instance for which the configuration is set. The ID can be found in the list displayed in Step 2, `"id":`
-orgId	(Optional). If left blank, the configuration is set for the default organization.

For example, `hznAdminTool failoverConfiguration –configType VIEW –configuration pod1vcs1.domain.com,pod2vcs1.hs.trcint.com –orgId 1 –serviceInstanceId 1`.

When you type this command for VMware Identity Manager instances in the secondary data center, reverse the order of the View Connection Servers. In this example, the command would be `hznAdminTool failoverConfiguration –configType VIEW –configuration pod2vcs1.hs.trcint.com, pod1vcs1.domain.com –orgId 1 –serviceInstanceId 103`

The resources failover database table is set up for each data center.

What to do next

To see the existing failover configuration for each of the View and Citrix-based resources, run `hznAdminTool failoverConfigurationList –configType <configtype> –<orgId)`.

The value for <configtype> is either VIEW or XENAPP. The following is an example output of `hznAdminTool failoverConfiguraitonList` with configType VIEW.

```
{"idOrganization":1,"serviceInstanceId":
52,"configType":"VIEW","configuration":"pod1vcs1.domain.com,pod2vcs1.domain.com"}
{"idOrganization":1,"serviceInstanceId":
103,"configType":"VIEW","configuration":"pod2vcs1.domain.com,pod1vcs1.domain.com"}
{"idOrganization":1,"serviceInstanceId":
154,"configType":"VIEW","configuration":"pod2vcs1.domain.com,pod1vcs1.domain.com"}
```

Configure Database for Failover

For VMware Identity Manager, database replication is configured so that data remains consistent across database servers within the primary data center and across to the secondary data center.

You must configure your external database for high availability. Configure a master and slave database architecture, where the slave is an exact replica of the master.

Refer to your external database documentation for information.

If you are using SQL Server Always On, use the hostname or IP address of the SQL Server listener when you configure the database in each VMware Identity Manager appliance. For example:

`jdbc:sqlserver://<listener_hostname>;DatabaseName=saas`

Failover to Secondary Data Center

When the primary data center fails, you can fail over to the secondary data center. To fail over, you need to modify the global load balancer or DNS record to point to the load balancer in the secondary data center.

Depending on your database setup, the VMware Identity Manager appliances in the secondary data center are either in read-only mode or in read-write mode. For all databases except SQL Server Always On, the VMware Identity Manager appliances are in read-only mode. Therefore, most administrator operations, like adding users or apps, or entitling users, are not available.

If you are using a SQL Server Always On deployment, the VMware Identity Manager appliances in the secondary data center are in read-write mode.

Using a DNS Record to Control Which Data Center is Active

If you use a Domain Name System (DNS) record to route user traffic in your data centers, the DNS record should point to a load balancer in the primary data center under normal operating situations.

If the primary data center becomes unavailable, the DNS record should be updated to point to the load balancer in the secondary data center.

When the primary data center becomes available again, the DNS record should be updated to point to the load balancer in primary data center.

Setting Time To Live in DNS Record

The time to live (TTL) setting determines how long before DNS related information is refreshed in the cache. For a seamless failover of View desktops and applications, make sure that the time to live (TTL) setting on the DNS records is short. If the TTL setting is set too long, users might not be able to access their View desktops and applications immediately after failover. To enable quick refresh of the DNS, set the DNS TTL to 30 seconds.

VMware Identity Manager Activities Not Available in Read-Only Mode

Using VMware Identity Manager in read-only mode is designed for high availability to allow end users access to the resources in their My Apps portal. Some activities in the VMware Identity Manager administration console and other administration services pages might not be available in read-only mode. Below is a partial list of common activities that are not available.

When VMware Identity Manager is running in read-only mode, activities related to changes in Active Directory or the database cannot be made and syncing to the VMware Identity Manager database does not work.

Administrative functions that require writing to the database are not available during this time. You must wait until VMware Identity Manager returns to read and write mode.

VMware Identity Manager Administration Console Read-Only Mode

The following are some of the limitations in the administration console in read-only mode.

- Adding, deleting, editing users and groups in the **Users & Groups** tab
- Adding, deleting, editing applications in the **Catalog** tab
- Adding, deleting, editing application entitlements
- Changing branding information
- Directory Sync to add, edit, delete users and groups
- Editing information about resources, including View, XenApp, and other resources
- Editing the Authentication Methods page

Note The connector components of the VMware Identity Manager appliances in the secondary data center appear in the administration console. Make sure that you do not select a connector from the secondary data center as the sync connector.

Virtual Appliance Configuration Pages Read-Only Mode

The following are some of the limitations in the Appliance Configuration pages in read-only mode

- Testing the database connection setup
- Changing the admin password in the Change Password page

End User Apps Portal Read-Only Mode

When VMware Identity Manager is in read-only mode, users can sign in to their VMware Identity Manager portal and access their resources. The following functionality in the end user portal is not available in read-only mode.

- Mark a resource as Favorite or unmark a resource as Favorite
- Add resources from the Catalog page or remove resources from the Launcher page
- Change their password from their apps portal page

VMware Identity Manager Windows Client Read-Only Mode

When VMware Identity Manager is in read-only mode, users cannot set up new Windows clients. Existing Windows clients continue to work.

Failback to Primary Data Center

In most failure scenarios, you can fail back to the primary data center once that data center is functioning again.

Procedure

1 Modify the global load balancer or the DNS record to point to the load balancer in the primary data center.

See "Using a DNS Record to Control Which Data Center is Active," on page 89.

2 Clear the cache in the secondary data center.

You can use REST APIs to clear the cache.

PATH: /SAAS/jersey/manager/api/removeAllCaches

Method: POST

Roles Allowed: OPERATOR only

Promoting Secondary Data Center to Primary Data Center

In case of an extended data center failure, the secondary data center can be promoted to primary.

For a SQL Server Always On deployment, no changes are required. For other database configurations, you need to edit the `runtime-config.properties` file in the VMware Identity Manager appliances in the secondary data center to configure the appliances for read-write mode.

Make these changes in each VMware Identity Manager appliance in the secondary data center.

Procedure

1 Using a ssh client, log in to the VMware Identity Manager appliance as the root user.

2 Open the `/usr/local/horizon/conf/runtime-config.properties` file for editing.

3 Change the `read.only.service=true` line to `read.only.service=false`.

4 Save the `runtime-config.properties` file.

5 Restart the Tomcat server on the appliance.

```
service horizon-workspace restart
```

Upgrading VMware Identity Manager with No Downtime

With a multi-data center deployment, you can upgrade VMware Identity Manager to the next version with no downtime. Use this suggested workflow for rolling updates.

Refer to the diagram in "Deploying VMware Identity Manager in a Secondary Data Center for Failover and Redundancy," on page 80 as you follow these steps.

Procedure

1 Switch routing on the Global LB to send the requests to the DC2 LB.

2 Stop database replication.

3 Update the vIDM1 virtual appliance, then update the vIDM2 virtual appliance, and then update the vIDM 3 virtual appliance.

4 Test updates using DC1-LB.

5 Once satisfied, switch Global LB to route requests to DC1 LB.

6 Update the vIDM4 virtual appliance, then update the vIDM5 virtual appliance, and then update the vIDM6 virtual appliance.

7 Test updates using DC2-LB.

8 Start database replication.

Installing Additional Connector Appliances

7

The connector is a part of the VMware Identity Manager service. When you install a VMware Identity Manager virtual appliance, a connector component is always included by default.

The connector performs the following functions.

- Syncs user and group data between your enterprise directory and the corresponding directory you create in the service.
- When used as an identity provider, authenticates users to the service.

  The connector is the default identity provider.

As a connector is already available as part of the service, in typical deployments you do not need to install an additional connector.

In some scenarios, however, you might need an additional connector. For example:

- If you have multiple directories of type Active Directory (Integrated Windows Authentication), you need a separate connector for each.

  A connector instance can be associated with multiple directories. A partition called the worker is created in the connector for each directory. However, you cannot have two workers of the Integrated Windows Authentication type in the same connector instance.
- If you want to manage users' access based on whether they sign in from an internal or external location.
- If you want to use certificate-based authentication but your load balancer is configured to terminate SSL at the load balancer. Certificate authentication requires SSL pass-through at the load balancer.

To install an additional connector, you perform the following tasks.

- Download the connector OVA package.
- Generate an activation token in the service.
- Deploy the connector virtual appliance.
- Configure connector settings.

Any additional connectors you deploy appear in the service user interface.

This chapter includes the following topics:

Generate Activation Code for Connector

Before you deploy the connector virtual appliance, generate an activation code for the new connector from the VMware Identity Manager service. The connector activation code is used to establish communication between the service and the connector.

Procedure

1 Log in to the VMware Identity Manager administration console.

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

3 Click **Setup**.

4 In the Connectors page, click **Add Connector**.

5 Enter a name for the new connector instance.

6 Click **Generate Activation Code**.

The activation code is displayed in the **Connector Activation Code** field.

7 Copy and save the connector activation code.

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

What to do next

Install the connector virtual appliance.

Deploy the Connector OVA File

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

Prerequisites

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

Procedure

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

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

Page	Description
Source	Browse to the OVA package location, or enter a specific URL.
OVA Template Details	Verify that you selected the correct version.
License	Read the End User License Agreement and click **Accept**.
Name and Location	Enter a name for the virtual appliance. The name must be unique within the inventory folder and can contain up to 80 characters. Names are case sensitive. Select a location for the virtual appliance.
Host / Cluster	Select the host or cluster to run the deployed template.
Resource Pool	Select the resource pool.
Storage	Select the location to store the virtual machine files.

Page	Description
Disk Format	Select the disk format for the files. For production environments, select a **Thick Provision** format. Use the **Thin Provision** format for evaluation and testing.
Network Mapping	Map the networks in your environment to the networks in the OVF template.
Properties	a In the **Timezone setting** field, select the correct time zone. b The Customer Experience Improvement Program checkbox is selected by default. VMware collects anonymous data about your deployment in order to improve VMware's response to user requirements. Deselect the checkbox if you do not want the data collected. c In the Host Name text box, enter the host name to use. If this is blank, reverse DNS is used to look up the host name. d To configure the static IP address for connector, enter the address for each of the following: Default Gateway, DNS, IP Address, and Netmask. IMPORTANT If any of the four address fields, including Host Name, are left blank, DHCP is used. To configure DHCP, leave the address fields blank.
Ready to Complete	Review your selections and click **Finish**.

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

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

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

What to do next

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

Configure Connector Settings

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

Prerequisites

- You have the activation code for the new connector. See "Generate Activation Code for Connector," on page 94.
- Ensure the connector appliance is powered on and you know the connector URL.
- Collect a list of passwords to use for the connector administrator, root account, and sshuser account.

Procedure

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

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

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

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

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

4 Click **Continue**.

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

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

The connector configuration is complete.

What to do next

In the service, set up your environment based on your needs. For example, if you added an additional connector because you want to sync two Integrated Windows Authentication directories, create the directory and associate it with the new connector.

Configure SSL certificates for the connector. See "Using SSL Certificates," on page 35.

Preparing to Use Kerberos Authentication on iOS Devices

8

When you initially deploy the VMware Identity Manager service, your existing Active Directory infrastructure is used for user authentication and management. You integrate the service with other authentication solutions such as Kerberos, Certificate, and RSA SecurID from the administration console. For Mobile SSO authentication on AirWatch managed iOS devices, you manually initialize the Key Distribution Center (KDC) in the appliance before you enable the authentication method from the administration console.

Kerberos authentication provides users, who are successfully signed in to their domain, access to their apps portal without additional credential prompts. To support iOS devices using Kerberos, VMware Identity Manager provides the built-in Kerberos authentication method, Mobile SSO for iOS, to access the KDC within the built-in identity provider without the use of a connector or a third-party system.

After you initialize the KDC and restart the service, create public DNS entries to allow the Kerberos clients to find the KDC.

To use the Mobile SSO for iOS authentication method, you must configure both AirWatch and the VMware Identity Manager service. See the VMware Identity Manager Administration Guide, Implementing Built-in Kerberos Authentication for AirWatch-Managed iOS Devices.

This chapter includes the following topics:

Pre- KDC Configuration Decisions

Before you initialize KDC in VMware Identity Manager, determine the realm name for the KDC server; whether subdomains are in your deployment, and whether to use default KDC server certificate or not.

Realm

The realm is the name of an administrative entity that maintains authentication data. Selecting a descriptive name for the Kerberos authentication realm is important. The realm name must be a part of a DNS domain that the enterprise can configure.

The realm name and the fully qualified domain name (FQDN) that is used to access the VMware Identity Manager service are independent. Your enterprise must control the DNS domains for both the realm name and the FQDN. The convention is to make the realm name the same as your domain name, entered in uppercase letters. Sometimes the realm name and domain are different. For example, a realm name is *EXAMPLE.NET*, and *idm.example.com* is the VMware Identity Manager FQDN. In this case, you define DNS entries for both *example.net* and *example.com* domains.

The realm name is used by a Kerberos client to generate DNS names. For example, when the name is example.com, the Kerberos related name to contact the KDC by TCP is *_kerberos._tcp.EXAMPLE.COM*.

Using Subdomains

The VMware Identity Manager service installed in an on-premises environment can use the VMware Identity Manager FQDN subdomain. If your VMware Identity Manager site accesses multiple DNS domains, configure the domains as location1.example.com; location2.example.com; location3.example.com. The subdomain value in this case is example.com, typed in lower case. To configure a subdomain in your environment work with your service support team.

Using KDC Server Certificates

When the KDC is initialized, by default a KDC server certificate and a self-signed root certificate are generated. The certificate is used to issue the KDC server certificate. This root certificate is included in the device profile so that the device can trust the KDC.

You can manually generate the KDC server certificate using an enterprise root or intermediate certificate. Contact your service support team for more details about this feature.

You download the KDC server root certificate from the VMware Identity Manager admin console to use in the AirWatch configuration of the iOS device management profile.

Initialize the Key Distribution Center in the Appliance

Before you can use the Mobile SSO for iOS authentication method, you must initialize the Key Distribution Center (KDC) in the VMware Identity Manager appliance.

To initialize KDC, you assign your identity manager hostname to the Kerberos realms. The domain name is entered in upper-case letters. If you are configuring multiple Kerberos realms, to help identify the realm, use descriptive names that end with your identity manager domain name. For example, SALES.MY-IDENTITYMANAGER.EXAMPLE.COM. If you configure subdomains, type the subdomain name in lower-case letters.

Prerequisites

VMware Identity Manager is installed and configured.

Realm name identified. See "Pre- KDC Configuration Decisions," on page 97.

Procedure

1 SSH into the VMware Identity Manager appliance as the root user.

2 Initialize the KDC. Enter `/etc/init.d/vmware-kdc init --realm {REALM.COM} --subdomain {sva-name.subdomain}`.

   For example, `/etc/init.d/vmware-kdc init --realm MY-IDM.EXAMPLE.COM --subdomain my-idm.example.com`

   If you are using a load balancer with multiple identity manager appliances, use the name of the load balancer in both cases.

3 Restart the VMWare Identity Manager service. Enter `service horizon-workspace restart`.

4 Start the KDC service. Enter `service vmware-kdc restart`.

What to do next

Create public DNS entries. DNS records must be provisioned to allow the clients to find the KDC. See "Creating Public DNS Entries for KDC with Built-In Kerberos," on page 99.

Creating Public DNS Entries for KDC with Built-In Kerberos

After you initialize KDC in VMware Identity Manager, you must create public DNS records to allow the Kerberos clients to find the KDC when the built-in Kerberos authentication feature is enabled.

The KDC realm name is used as part of the DNS name for the VMware Identity Manager appliance entries that are used to discover the KDC service. One SRV DNS record is required for each VMware Identity Manager site and two A address entries.

Note The AAAA entry value is an IPv6 address that encodes an IPv4 address. If the KDC is not addressable via IPv6 and an IPv4 address is used, the AAAA entry might have to be specified in a strict IPv6 notation as `::ffff:175c:e147` on the DNS server. You can use an IPv4 to IPv6 conversion tool, such as one available from Neustar.UltraTools, to convert IPv4 to IPv6 address notation.

Example: DNS Record Entries for KDC

In this example DNS record, the realm is `EXAMPLE.COM`; the VMware Identity Manager fully qualified domain name is `idm.example.com`, and the VMware Identity Manager IP address `1.2.3.4`.

```
idm.example.com.               1800 IN  AAAA         ::ffff:1.2.3.4

idm.example.com.               1800 IN  A            1.2.3.4

_kerberos._tcp.EXAMPLE.COM           IN  SRV  10  0   88 idm.example.com.

_kerberos._udp.EXAMPLE.COM           IN  SRV  10  0   88 idm.example.com.
```

Troubleshooting Installation and Configuration 9

The troubleshooting topics describe solutions to potential problems you might encounter when installing or configuring VMware Identity Manager.

This chapter includes the following topics:

Users Unable to Launch Applications or Incorrect Authentication Method Applied in Load-Balanced Environments

Users are unable to launch applications from the Workspace ONE portal or the wrong authentication method is applied in a load-balanced environment.

Problem

In a load-balanced environment, problems such as the following might occur:

- Users are unable to launch applications from the Workspace ONE portal after they log in.
- The wrong authentication method is presented to users for step-up authentication.

Cause

These problems can occur if access policies are determined incorrectly. The client IP address determines which access policy is applied during login and during application launch. In a load-balanced environment, VMware Identity Manager uses the X-Forwarded-For header to determine the client IP address. In some cases, an error might occur.

Solution

Set the `service.numberOfLoadBalancers` property in the `runtime-config.properties` file in each of the nodes in your VMware Identity Manager cluster. The property specifies the number of load balancers fronting the VMware Identity Manager instances.

Note Setting this property is optional.

1 Log in to the VMware Identity Manager appliance.

2 Edit the `/usr/local/horizon/conf/runtime-config.properties` file and add the following property:

```
service.numberOfLoadBalancers numberOfLBs
```

where *numberOfLBs* is the number of load balancers fronting the VMware Identity Manager instances.

3 Restart the workspace appliance.

```
service horizon-workspace restart
```

Group Does Not Display Any Members after Directory Sync

Directory sync completes successfully but no users are displayed in synced groups.

Problem

After a directory is synced, either manually or automatically based on the sync schedule, the sync process completes successfully but no users are displayed in synced groups.

Cause

This problem occurs when you have two or more nodes in a cluster and there is a time difference of more than 5 seconds between the nodes.

Solution

1 Ensure that there is no time difference between the nodes. Use the same NTP server across all nodes in the cluster to synchronize the time.

2 Restart the service on all the nodes.

```
service horizon-workspace restart
```

3 (Optional) In the administration console, delete the group, add it again in the sync settings, and sync the directory again.

Troubleshooting Elasticsearch and RabbitMQ

Use this information to troubleshoot problems with Elasticsearch and RabbitMQ in a cluster environment. Elasticsearch, a search and analytics engine used for auditing, reports, and directory sync logs, and RabbitMQ, a messaging broker, are embedded in the VMware Identity Manager virtual appliance.

Troubleshooting Elasticsearch

You can verify the health of Elasticsearch by using the following command in the VMware Identity Manager appliance.

```
curl 'http://localhost:9200/_cluster/health?pretty'
```

The command should return a result similar to the following.

```
        {
  "cluster_name" : "horizon",
  "status" : "green",
  "timed_out" : false,
  "number_of_nodes" : 3,
  "number_of_data_nodes" : 3,
  "active_primary_shards" : 20,
  "active_shards" : 40,
  "relocating_shards" : 0,
  "initializing_shards" : 0,
  "unassigned_shards" : 0,
```

```
  "delayed_unassigned_shards" : 0,
  "number_of_pending_tasks" : 0,
  "number_of_in_flight_fetch" : 0
}
```

If Elasticsearch does not start correctly or its status is red, follow these steps to troubleshoot.

1 Ensure port 9300 is open.

   a Update node details by adding the IP addresses of all nodes in the cluster to the `/usr/local/horizon/scripts/updateiptables.hzn` file:

   ```
   ALL_IPS="node1IPadd node2IPadd node3IPadd"
   ```

   b Run the following script on all nodes in the cluster.

   ```
   /usr/local/horizon/scripts/updateiptables.hzn
   ```

2 Restart Elasticsearch on all nodes in the cluster.

   ```
   service elasticsearch restart
   ```

3 Check logs for more details.

   ```
   cd /opt/vmware/elasticsearch/logs
   ```

   ```
   tail –f horizon.log
   ```

Troubleshooting RabbitMQ

You can verify the health of RabbitMQ by using the following command in the VMware Identity Manager appliance.

```
rabbitmqctl cluster_status
```

The command should return a result similar to the following.

```
Cluster status of node 'rabbitmq@node3' ...
[{nodes,[{disc,['rabbitmq@node2','rabbitmq@node3']}]},
 {running_nodes,['rabbitmq@node3']},
 {cluster_name,<<"rabbitmq@node2.example.com">>},
 {partitions,[]},
 {alarms,[{'rabbitmq@node3',[]}]}]
```

If RabbitMQ does not start or the health URL https://hostname/SAAS/API/1.0/REST/system/health/ shows `"MessagingConnectionOk":"false"`, follow these steps to troubleshoot.

1 Ensure ports 4369, 5700, 25672 are open. To open ports:

   a Create the file by using this command:

   ```
   touch /usr/local/horizon/conf/flags/enable.rabbitmq
   ```

   b Run the following script:

   ```
   /usr/local/horizon/scripts/updateiptables.hzn
   ```

2 Restart RabbitMQ.

   a Kill any existing `rabbitmq` processes.

   b `rabbitmqctl stop`

   c `rabbitmq-server –detached`

3 You may need to restart the VMware Identity Manager service if RabbitMQ does not start gracefully.

   ```
   service horizon-workspace restart
   ```

Index