Installing and Configuring VMware Identity Manager for Linux

VMware Identity Manager 3.3

vmware by Broadcom

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

https://docs.vmware.com/

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

Contents

About Installing and Configuring VMware Identity Manager for Linux

Installing and Configuring VMware Identity Manager for Linux provides information about installing and configuring the VMware Identity Manager Linux-based virtual appliance on premises. 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 Web applications, Horizon applications and desktops, and Citrix published resources. The guide also explains how to configure your deployment for high availability.

Installing and Configuring VMware Identity Manager for Linux provides information about deploying the VMware Identity Manager virtual appliance in the internal network. To deploy VMware Identity Manager in the DMZ, see *Deploying VMware Identity Manager in the DMZ*.

Intended Audience

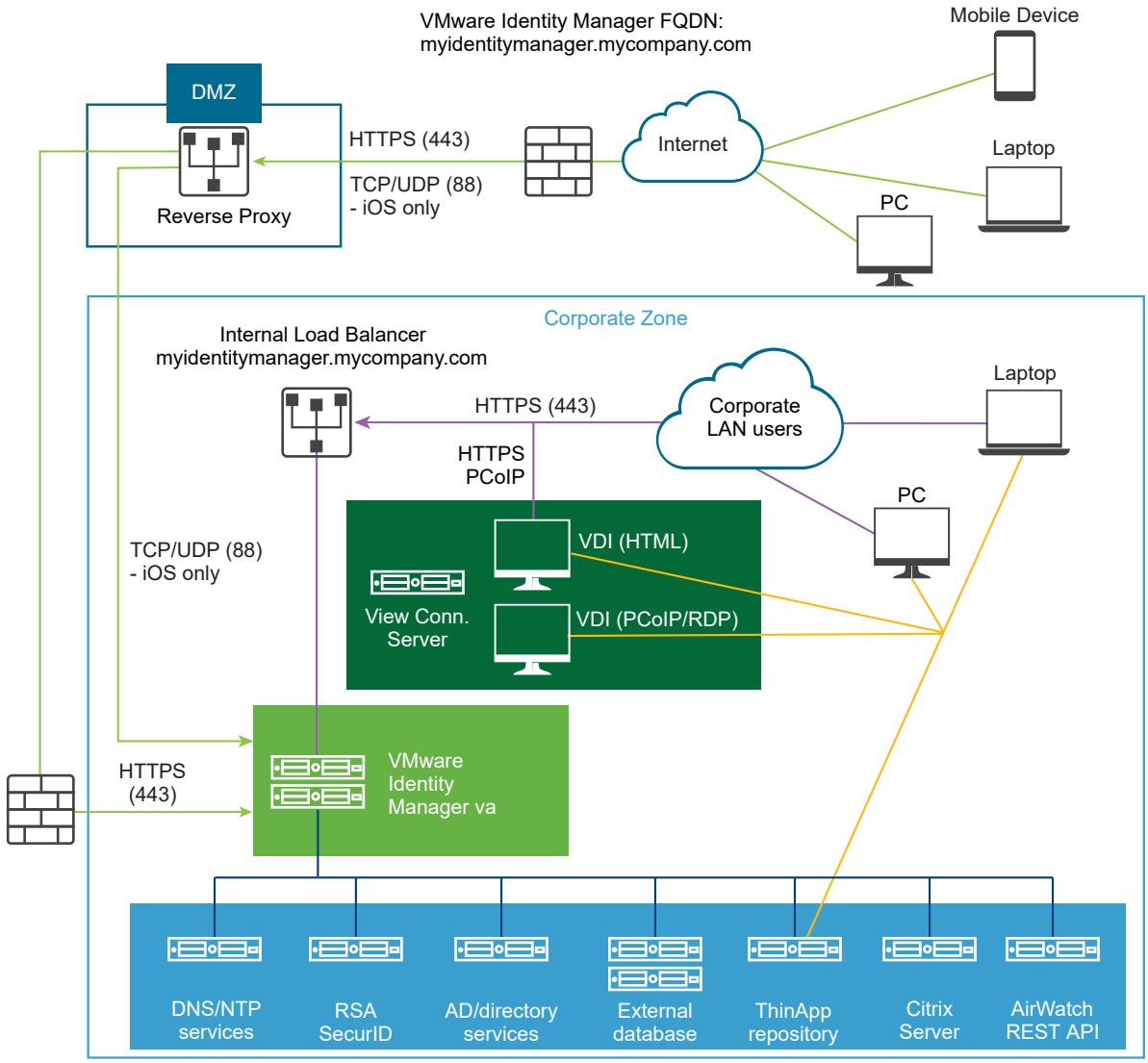
This information is intended for administrators of VMware Identity Manager. The information is written for experienced Windows and Linux system administrators who are familiar with VMware technologies, particularly vCenter™, ESX™, and vSphere®, networking concepts, Active Directory servers, databases, backup and restore procedures, Simple Mail Transfer Protocol (SMTP), and NTP servers. 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 Workspace ONE UEM deployment, the Workspace ONE UEM REST APIs could be in the cloud or on premises.

Read the following topics next:

- System and Network Configuration Requirements
- Preparing to Deploy VMware Identity Manager
- Customer Experience Improvement Program

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:

- 5.5 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.

Compatibility Between VMware Identity Manager Service and Connector

With the VMware Identity Manager on premises service, you can use supported connector versions that are either the same or lower than the service version. For example, with the VMware Identity Manager 3.3 service, you can use connector 2018.8.1.0, the connector released with the 3.3 service, and earlier versions. You cannot use a connector version that is higher than the service version. For example, you cannot use the 19.03 connector with the 3.3 service. Using the latest compatible version of the connector is recommended.

For information on supported versions, see https://www.vmware.com/support/policies/lifecycle.html.

Hardware Sizing 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, standalone connectors, 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	50,000-100,000
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 Microsoft SQL database to store and organize server data.

For information about the Microsoft SQL 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. The exact specifications needed for your SQL server depend on the size and needs of your deployment.

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

The SQL Server AlwaysOn capability is a combination of failover clustering and database mirroring combined with log shipping for high availability. AlwaysON allows for multiple read copies of your database and a single read-write copy for operations. If your deployment environment has the bandwidth to support the traffic generated, the VMware Identity Manager database supports AlwaysON.

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. VMware Unified Access Gateway 2.8 and later supports reverse proxy functionality to allow users to securely access the VMware Identity Manager unified catalog remotely. Unified Access Gateway can be deployed in the DMZ behind the load balancers front-ending the VMware Identity Manager appliance.

Port Requirements

Ports used in the server configuration are described here. Your deployment might include only a subset of these ports. For example:

- 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	Protocol	Source	Target	Description
443	HTTPS	Load Balancer	VMware Identity Manager machine	
443	HTTPS	VMware Identity Manager	Load Balancer	Needed to validate the load balancer FQDN when it is set.
443, 8443	HTTPS/HTTP	VMware Identity Manager machine	VMware Identity Manager machine	For all VMware Identity Manager instances in a cluster, and across clusters in different data centers.
443	HTTPS	Browsers	VMware Identity Manager machine	
443, 80	HTTPS, HTTP	VMware Identity Manager machine	vapp-updates.vmware.com	Access to the upgrade server
443	HTTPS	VMware Identity Manager machine	discovery.awmdm.com	Access for Workspace ONE application autodiscovery

Port	Protocol	Source	Target	Description
443	HTTPS	VMware Identity Manager machine	catalog.vmwareidentity.com	Access to Cloud Catalog
8443	HTTPS	Browsers	VMware Identity Manager machine	Administrator Port
25	SMTP	VMware Identity Manager machine	SMTP	Port to relay outbound mail
389 636 3268 3269	LDAP LDAPS MSFT-GC MSFT-GC-SSL	VMware Identity Manager machine	Active Directory	Default values are shown. These ports are configurable.
445	TCP	VMware Identity Manager machine	VMware ThinApp repository	Access to the ThinApp repository
5500	UDP	VMware Identity Manager machine	RSA SecurID system	Default value is shown. This port is configurable.
53	TCP/UDP	VMware Identity Manager machine	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, 445	TCP/UDP	VMware Identity Manager machine	Domain controller	
9300	TCP	VMware Identity Manager machine	VMware Identity Manager machine	Audit needs
54328	UDP			
5701	TCP	VMware Identity Manager machine	VMware Identity Manager machine	Hazelcast cache
40002 40003	TCP	VMware Identity Manager machine	VMware Identity Manager machine	Ehcache
1433	TCP	VMware Identity Manager machine	Database	Microsoft SQL default port is 1433
443		VMware Identity Manager	Horizon server	Access to Horizon server
80, 443	TCP	VMware Identity Manager	Integration Broker server	Connection to the Integration Broker. Port option depends on whether a certificate is installed on the Integration Broker server

Port	Protocol	Source	Target	Description
443	HTTPS	VMware Identity Manager	Workspace ONE UEM (AirWatch) REST API	For device compliance checking and for the AirWatch Cloud Connector password authentication method, if that is used.
88	UDP	Unified Access Gateway	VMware Identity Manager machine	UDP port to open for mobile SSO
5262	TCP	Android mobile device	Workspace ONE UEM (AirWatch) HTTPS proxy service	Workspace ONE UEM (AirWatch) Tunnel client routes traffic to the HTTPS proxy for Android devices.
88	UDP	iOS mobile device	VMware Identity Manager machine	Port used for Kerberos traffic from iOS devices to the hosted cloud KDC service.
443	HTTPS/TCP			
514	UDP	VMware Identity Manager machine	syslog server	UDP For external syslog server, if configured
88	UDP	VMware Identity Manager machine	Hybrid KDC Server in the cloud. Hostname is kdc.<realm>. For example, kdc.op.vmwareidentity.com	UDP port used to authenticate iOS Mobile SSO auth adapter configuration updates that are saved to the cloud KDC service. This port is only used if the Hybrid KDC iOS Mobile SSO feature is used.

Supported Directories

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

- The Active Directory environment can consist of a single Active Directory domain, multiple domains in a single Active Directory forest, or multiple domains across multiple Active Directory forests.

VMware Identity Manager supports Active Directory on Windows 2008, 2008 R2, 2012, 2012 R2, 2016, and 2019 with a Domain functional level and Forest functional level of Windows 2003 and later.

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

Supported Web Browsers to Access the VMware Identity Manager Console

The VMware Identity Manager console is a web-based application you use to manage your tenant. You can access the VMware Identity Manager console from the latest versions of Mozilla Firefox, Google Chrome, Safari, Microsoft Edge, and Internet Explorer 11.

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

Supported Browsers to Access the Workspace ONE Portal

End users can access the Workspace ONE portal from the following browsers.

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

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

What to read next

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

Note You must use a static IP address and it must have a PTR and an A record defined in the DNS.

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.

Planning for Kerberos Authentication

If you plan to set up Kerberos authentication, note the following requirements:

- In a scenario where you use the embedded connector in VMware Identity Manager for Kerberos authentication, the VMware Identity Manager host name must match the Active Directory domain to which VMware Identity Manager is joined. For example, if the Active Directory domain is sales.example.com, the VMware Identity Manager host name must be *vidmhost*.sales.example.com.

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

- In a scenario where you use external connectors for Kerberos authentication, the connector host name must match the Active Directory domain to which the connector is joined. For example, if the Active Directory domain is sales.example.com, the connector host name must be *connectorhost*.sales.example.com.

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

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.

What to read next

Database Options with VMware Identity Manager

Set up VMware Identity Manager with the internal PostgreSQL database or an external Microsoft SQL database to store and organize server data. Both options can provide high availability.

An internal PostgreSQL database is embedded in the VMware Identity Manager appliance and is configured and ready to use by default. To achieve high availability with the internal PostgreSQL database, you must leverage vRealize Suite Lifecycle Manager. See the *vRealize Suite Lifecycle Manager Installation, Upgrade, and Management* guide.

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 the Microsoft SQL database server to set up a high availability external database environment. See Create the VMware Identity Manager Service Database.

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 *Directory Integration with VMware Identity Manager* 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	If you plan to set up Kerberos authentication, note the following conditions. In a scenario where you use the VMware Identity Manager connector for Kerberos authentication, the connector host name must match the Active Directory domain to which the connector is joined. For example, if the Active Directory domain is sales.example.com, the connector host name must be *connectorhost*.sales.example.com. If you cannot assign a hostname that matches the Active Directory domain structure, you need to configure the connector and Active Directory manually. See the Knowledge Base for information.

Network Information for VMware Identity Manager Appliance

Table 1-4. Network Information Checklist

Information to Gather	List the Information
IP address	**Note** You must use a static IP address and it must have a PTR and an A record defined in the DNS.
DNS host name for each node	
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 service.

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 VMware Identity Manager 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	

What to read next

Customer Experience Improvement Program

VMware's Customer Experience Improvement Program ("CEIP") provides VMware with information that enables VMware to improve its products and services, to fix problems, and to advise you on how best to deploy and use our products. As part of the CEIP, VMware collects technical information about your organization's use of VMware products and services on a regular basis in association with your organization's VMware license key(s). This information does not personally identify any individual.

If you prefer not to participate in VMware's CEIP for this product, uncheck the box when you install VMware Identity Manager.

You can also join or leave the CEIP for this product at any time after installation.

Note If your network is configured to access the Internet through HTTP proxy, to send the data collected through CEIP to VMware, you must adjust the proxy settings in VMware Identity Manager.

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.

Read the following topics next:

- Install the VMware Identity Manager OVA File
- (Optional) Add IP Pools
- Configure VMware Identity Manager Settings
- Adding Whitelist IP Addresses to Your External Firewall
- Setting Proxy Server Settings for VMware Identity Manager
- Enter the License Key

Install the VMware Identity Manager OVA File

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

Note 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.

Procedure

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

2 Log in to 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.

Page	Description
Properties	■ **Timezone setting** Select the correct time zone. ■ **Join the VMware Customer Experience Improvement Program** This product participates in VMware's Customer Experience Improvement Program ("CEIP"). Details regarding the data collected through CEIP and the purposes for which it is used by VMware are set forth at the Trust & Assurance Center at https://www.vmware.com/solutions/trustvmware/ceip.html. If you prefer not to participate in VMware's CEIP for this product, uncheck the box. You can also join or leave the CEIP for this product at any time after installation. **Note** If your network is configured to access the Internet through HTTP proxy, to send the data collected through CEIP to VMware you must adjust the proxy settings in the VMware Identity Manager virtual appliance. See Setting Proxy Server Settings for VMware Identity Manager. ■ **Host Name (FQDN)** Enter the host name to use. If this is blank, reverse DNS is used to look up the host name. ■ **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.
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 virtual appliance is initialized. When the 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 console 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.IdentityManager
   - vami.netmask0.IdentityManager
   - vami.gateway.IdentityManager

   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.

Results

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 instance 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.

Make sure that your run the Setup wizard using the fully qualified host name. Do not enter the IP address as the name.

Prerequisites

- The VMware Identity Manager machine is powered on.
- The external database is configured and the external database connection information is available. Before you run the Setup wizard, verify that the database configuration is correct. See Create the VMware Identity Manager Service Database for information.
- Before setting up the directory, review *Directory Integration with VMware Identity Manager* 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 are 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 and users you want to add to VMware Identity Manager.

  Group names are synced to the directory immediately. Members of a group do not sync until the group is entitled to resources or added to a policy rule. Users who need to authenticate before group entitlements are configured should be added directly during the initial configuration.

Procedure

1. Go to the VMware Identity Manager URL that was displayed when you finished the installation. Enter the fully qualified domain name (FQDN). For example, `https://hostname.example.com`.
2. Accept the certificate, if prompted.

   You can update the certificate after the initial set up.
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 Configure VMware Identity Manager to Use an External Database

- 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 VMware Identity Manager console to set up the Active Directory or LDAP directory connection.

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

You are logged in as a local admin and the Directories page appears. Before you add a directory, ensure that you review *Directory Integration with VMware Identity Manager* 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.

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 #unique_17.

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. ■ 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" in *Directory Integration with VMware Identity Manager*. ■ If the Active Directory requires access over SSL, select the **This Directory requires all connections to use SSL** check box in the **Certificates** section and copy and paste the Active Directory Root CA certificate into the **SSL Certificate** field.

Option	Description
	Ensure the certificate is in PEM format and include the "BEGIN CERTIFICATE" and "END CERTIFICATE" lines. **Note** If the Active Directory requires SSL and you do not provide the certificate, you cannot create the directory. 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" in *Directory Integration with VMware Identity Manager* for more information.

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 **Bind User Details** section, enter the user name and password of the bind user who has permission to query users and groups for the required domains. For the user name, enter the sAMAccountName, for example, jdoe. If the bind user's domain is different from the Join Domain entered above, enter the user name as sAMAccountName@domain, where domain is the fully-qualified domain name. For example, jdoe@example.com. **Note** Using a Bind user account with a non-expiring password is recommended.

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`**

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

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.

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

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

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

b (Optional) To exclude users, create a filter to exclude some types of users.

You select the user attribute to filter by, the query rule, and the value.

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.

Results

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 4 Advanced Configuration for the VMware Identity Manager Appliance.

Adding Whitelist IP Addresses to Your External Firewall

When you configure VMware identity Manager with an external firewall, whitelist the IP address ranges or URLs for the following VMware Identity Manager services to provide access to that service.

Use the **nslookup** command or another command-line tool to query the Domain Name System to obtain the IP addresses to add to your external firewall whitelist.

Service	Domain Name System	Description
VMware Identity Manager Catalog	`catalog.vmwareidentity.com`	To make sure that the content of the catalog can be accessed, add the URLs from the list to the whitelist. That content is also delivered through AWS CloudFront CDN, which maintains its own list of public IP addresses. See http://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/LocationsOfEdgeServers.html.
VMware Verify	`vmware.authy.com` `api.authy.com`	If VMware Verify is configured as an authentication method, add the URLS from these lists to the whitelist.

Service	Domain Name System	Description
Hybrid KDC	`kdc.op.<vmwareidentity.xxx>`	When hybrid KDC is configured for your VMware Identity Manager on-premises operation, select one of the following domains to look up the URLS. ■ vmwareidentity.ca ■ vmwareidentity.com ■ vmwareidentity.eu ■ vmwareidentity.co.uk ■ vmwareidentity.de ■ vmwareidentity.com.au ■ vmwareidentity.asia
Updates from VMware Identity Manager	`vapp-updates.vmware.com`	To receive VMware Identity Manager updates and to download patches from the VMware Update Manager, add the URLs from the list to the whitelist.

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.

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
```

Results

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 console.
2. Select the **Appliance Settings** tab, then click **License**.
3. In the License Settings page, enter the license key and click **Save**.

Managing VMware Identity Manager Configuration Settings

3

After the initial configuration of VMware Identity Manager is complete, you can go to the VMware Identity Manager console pages to install certificates, manage passwords, and download log files. You can also update the database, change the Identity Manager FQDN, and configure an external syslog server.

The configuration settings pages are available from the Appliance Settings tab in the identity manager console.

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 Create the VMware Identity Manager Service Database.
Install SSL Certificates	On the tabs on this page, you can install an SSL certificate for VMware Identity Manager, download the self-signed VMware Identity Manager root certificate, and install trusted root certificates. For example, if VMware Identity Manager is configured behind a load balancer, you can install the load balancer's root certificate. **Note** The **Passthrough Certificate** tab is used only when certificate authentication is configured on the embedded connector in a DMZ deployment scenario. See *Deploying VMware Identity Manager in the DMZ* for information. See Using SSL Certificates.
Identity Manager FQDN	On this page, you can view or change the VMware Identity Manager FQDN. The 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 Configure a Syslog Server.
Change Password	On this page, you can change the VMware Identity Manager admin user password.

Page Name	Setting Description
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	You can download the logs in a zip file. See Log File Information.

You can also modify the connector URL. See Modifying the Connector URL.

Read the following topics next:

- Change Appliance Configuration Settings
- Create the VMware Identity Manager Service Database
- Using SSL Certificates
- Modifying the VMware Identity Manager Service URL
- Modifying the Connector URL
- Configure a Syslog Server
- Log File Information
- Manage Your Appliance Passwords
- Configure SMTP Settings

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 VMware Identity Manager 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.

Create the VMware Identity Manager Service Database

The VMware Identity Manager service requires a database to store and organize server data.

You can use the internal PostgreSQL database or an external Microsoft SQL database. Both options can provide high availability.

An internal PostgreSQL database is embedded in the VMware Identity Manager appliance and is configured and ready to use by default. To achieve high availability with the internal PostgreSQL database, you must leverage vRealize Suite Lifecycle Manager. See the *vRealize Suite Lifecycle Manager Installation, Upgrade, and Management* guide.

To use an external Microsoft SQL database, your database administrator must prepare an empty Microsoft SQL Server database and schema before you install VMware Identity Manager. When you connect to the Microsoft SQL server, you enter the name of the instance you want to connect to and the authentication mode. You can select either Windows Authentication mode and specify the domain\username or SQL Server Authentication mode and specify the local user name and password.

You 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.

Configure the Microsoft SQL Database with Windows Authentication Mode

To use a Microsoft SQL database for the VMware Identity Manager, you must create a new database in the Microsoft SQL server. During setup, you must select an authentication mode for the database. If you select Windows Authentication, when you create the database, you enter the user name and domain. The user name and domain is entered as `domain\username`.

When you run the Microsoft SQL commands, you create a database on the Microsoft SQL server, enter the database name, add the login user credentials, and create the schema. The schema name is **saas**.

Note The default collation is case-sensitive.

Prerequisites

- Supported version of the Microsoft SQL server installed as an external database server.
- Load balancing implementation configured.
- Windows Authentication selected as the authentication mode.
- 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 To create the database with the default schema named **saas**, enter the following commands in the editor window.

```
/*
Values within angle brackets (< >) are example values. When replacing the example value,
remove the angle brackets. The database name is case sensitive. Make sure you enter the
database name the same in all instances.
*/


CREATE DATABASE <saasdb>
COLLATE Latin1_General_CS_AS;
ALTER DATABASE <saasdb> SET READ_COMMITTED_SNAPSHOT ON;
GO

IF NOT EXISTS
(SELECT name
FROM master.sys.server_principals
WHERE name=N'<domain\username>')
BEGIN
CREATE LOGIN [<domain\username>] FROM WINDOWS;
END
GO

USE <saasdb>;
IF EXISTS (SELECT * FROM sys.database_principals WHERE name=N'<domain\username>')
DROP USER [<domain\username>]
GO

CREATE USER [<domain\username>] FOR LOGIN [<domain\username>]
WITH DEFAULT_SCHEMA=saas;
GO

CREATE SCHEMA saas AUTHORIZATION "<domain\username>"
GRANT ALL ON DATABASE::<saasdb> TO "<domain\username>";
GO

ALTER ROLE db_owner ADD MEMBER "<domain\username>";
GO
```

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

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

The server role used to grant server-wide security privileges is set to **public**. The database role membership is **db_owner**. Do not set any other roles.

Results

When you install the VMware Identity Manager for Windows, you select this database server instance to connect to. After the installation, the JDBC URL and the user name and password created for the database are configured in the Database Connection Setup page in the VMware Identity Manager server. See Configure VMware Identity Manager to Use an External Database

Configure Microsoft SQL Database Using Local SQL Server Authentication Mode

To use a Microsoft SQL database for the VMware Identity Manager, you must create a new database in the Microsoft SQL server. During setup, you must select an authentication mode for the database. If you select SQL Server Authentication, when you create the database, you enter a local user name and password.

When you run the Microsoft SQL commands, you create a database on the Microsoft SQL server, enter the database name, add the login user credentials, and create the schema. The schema is named **saas**.

Note The default database collation is case-sensitive.

Prerequisites

- Supported version of the Microsoft SQL server installed as an external database server.
- Load balancing implementation configured.
- SQL Server Authentication selected as the authentication mode.
- 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. To create the database with the default schema named **saas**, enter the following commands in the editor window.

```
/*
Values within angle brackets (< >) are example values. When replacing the example value,
remove the angle brackets. The database name is case sensitive. Make sure you enter the
database name the same in all instances.
*/


CREATE DATABASE <saasdb>
COLLATE Latin1_General_CS_AS;
```

```
ALTER DATABASE <saasdb> SET READ_COMMITTED_SNAPSHOT ON;
GO

BEGIN
CREATE LOGIN <loginusername> WITH PASSWORD = N'<password>';
END
GO

USE <saasdb>;
IF EXISTS (SELECT * FROM sys.database_principals WHERE name=N'<loginusername>')
DROP USER [<loginusername>]
GO

CREATE USER [<loginusername>] FOR LOGIN [<loginusername>]
WITH DEFAULT_SCHEMA=saas;
GO

CREATE SCHEMA saas AUTHORIZATION <loginusername>
GRANT ALL ON DATABASE::<saasdb> TO <loginusername>;
GO

ALTER ROLE [db_owner] ADD MEMBER <loginusername>;
GO
```

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

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

The server role used to grant server-wide security privileges is set to **public**. The database role membership is **db_owner**. Do not set any other roles.

Results

When you install the VMware Identity Manager for Windows, you select this database server instance to connect to. After the installation, the JDBC URL and the user name and password created for the database are configured in the Database Connection Setup page in the VMware Identity Manager server. See Configure VMware Identity Manager to Use an External Database

Confirm Microsoft SQL Database Is Correctly Configured

To confirm that the Microsoft SQL database is configured correctly to work with VMware Identity Manager, the following verification script runs after the database is configured.

Prerequisites

The Microsoft SQL database is created for the VMware Identity Manager service.

Procedure

1 Log in to the Microsoft SQL Server Management Studio session with the <saasdb> login user name and password that was created in the script you used to create the database.

The editor window appears.

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

3 Run the following commands. Edit the commands as required.

```
 execute as user = 'domain\username'


/* Check if user is db owner. Return true */
SELECT IS_ROLEMEMBER('db_owner') as isRoleMember

/* Make sure user is not sysadmin. Should return false */
SELECT IS_SRVROLEMEMBER('sysadmin')  as isSysAdmin

/* check if saas schema exists, should be not null */
SELECT SCHEMA_ID('saas') as schemaId

/* check schema owner, should be user provided to installer */
SELECT SCHEMA_OWNER FROM INFORMATION_SCHEMA.SCHEMATA where SCHEMA_NAME='saas'

/* check if saas is user default schema, should return saas */
SELECT SCHEMA_NAME() as SchemaName

/* check db collation, should return Latin1_General_CS_AS */
SELECT DATABASEPROPERTYEX('<saasdb>', 'Collation') AS Collation

/* check if read committed snapshot is on, should return true */
SELECT is_read_committed_snapshot_on FROM sys.databases WHERE name='<saasdb>'
```

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

If the configuration is not correct, error messages are displayed. Before continuing to configure the VMware Identity Manager service to use the external Microsoft SQL database, correct the problems described in the error messages.

Configure VMware Identity Manager to Use an External Database

After you create the Microsoft SQL database, if the external database you created is not automatically configured in VMware Identity Manager, you configure VMware Identity Manager to use the database in the Appliance Settings page.

Prerequisites

- The database with the saas schema created in Microsoft SQL server as the external database server. For information about specific versions that VMware Identity Manager supports, see the VMware Product Interoperability Matrixes.

Procedure

1 In the VMware Identity Manager 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 Enter the JDBC URL of the Microsoft SQL database server.

Authentication Mode	JDBC URL String
Windows Authentication (domain\user)	`jdbc:jtds:sqlserver://<hostname_or_IP_address:port#>/<saasdb>;integratedSecurity=true;domain=<domainname>;useNTLMv2=true`
SQL Server Authentication (local user)	`jdbc:sqlserver://<hostname_or_IP_address:port#>;DatabaseName=<saasdb>`

Note To enable SQL Server Always on capability, MultiSubNetFailover to set to True in the SQL. The JDBC URL string is

```
jdbc:jtds:sqlserver://<hostname_or_IP_address:port#>/<saasdb>;integratedSecurity=true;domain=<domainname>;useNTLMv2=true;multiSubnetFailover=true
```

b Enter the loginusername and password configured when you created the database. SeeConfigure Microsoft SQL Database Using Local SQL Server Authentication Mode

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

What to do next

(Optional) Change the db_owner database role membership privileges. See Change Database-Level Roles.

Change Database-Level Roles

When the saas schema is used to create the Microsoft SQL database for the VMware Identity Manager service, the database role membership is granted to the db_owner role. Members of the db_owner fixed database role can perform all configuration and maintenance activities on the database.

After the database is set up and configured in the VMware Identity Manager service, you can revoke access to db_owner and add db_datareader and db_datawriter as the database roles. Members of the db_datareader role can read all data from all user tables. Member of the db_datawriter role can add, delete, or change data in all user tables.

Note If you revoke access to db_owner, make sure that the db_owner role is granted back before you start an upgrade to a new version of VMware Identity Manager.

Prerequisites

User role for the Microsoft SQL Server Management Studio as sysadmin or as a user account with sysadmin privileges.

Procedure

1. In the Microsoft SQL Server management Studio session as an admin with sysadmin privileges, connect to the database instance <saasdb> for VMware Identity Manager.
2. Revoke the role **db_owner** on the database, enter the following command

Authentication Mode	Command
Windows Authentication (domain\user)	`ALTER ROLE db_owner DROP MEMBER <domain\username>;`
SQL Server Authentication (local user)	`ALTER ROLE db_owner DROP MEMBER <loginusername>;`

3. Add **db_datawriter** and **db_datareader** role membership to the database.

Authentication Mode	Command

Windows Authentication (domain\user)	`ALTER ROLE db_datawriter ADD MEMBER <domain\username>;`
	`GO`
	
	`ALTER ROLE db_datareader ADD MEMBER <domain\username>;`
	`GO`

SQL Server Authentication (local user)	`ALTER ROLE db_datawriter ADD MEMBER <loginusername>;`
	`GO`
	`ALTER ROLE db_datareader ADD MEMBER <loginusername>;`
	`GO`

Administering the Internal Database

The internal Postgres database is embedded in the VMware Identity Manager appliance and is configured and ready to use by default.

You can configure the internal PostgreSQL database for high availability if your deployment leverages vRealize Suite Lifecycle Manager. See the *vRealize Suite Lifecycle Manager Installation, Upgrade, and Management* guide.

When 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`.

Change SQL Server Database Auto Growth Settings

When you create the database, the default settings for auto growing is 1 MB for data files. The auto growth setting for the VMware Identity Manager database must be increased to 128 MB.

To see the vIDMDB database file auto growth setting, navigate to **DataBase Properties > Files**. The setting is displayed in the **Autogrowth / Maxsize** column.

Procedure

1. Log in to the Microsoft SL server Management Studio session as the sysadmin or a user account with sysadmin privileges.
2. In the toolbar, click **New Query**.
3. To change the auto growth setting, run the following command.

```
ALTER DATABASE <saasdb>

        MODIFY FILE ( NAME = N'<saasdb>', FILEGROWTH = 128MB )

GO
```

Results

The auto growth setting is changed to 128 MB.

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 obtain and install SSL certificates signed by a public Certificate Authority (CA) in your production environment.

A 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.

You can install a signed CA certificate from the **Appliance Settings > Manage Configuration > Install SSL Certificates > Server Certificates** page.

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 service. The clients can include end user machines, load balancers, proxies, and so on. You can download the root CA from the **Install SSL Certificates > Server Certificates** page.

Installing an SSL Certificate for the VMware Identity Manager Service

When the VMware Identity Manager service is installed, a default SSL server certificate is generated. You can use this self-signed certificate for testing purposes. However, VMware strongly recommends that you use SSL certificates signed by a public Certificate Authority (CA) for your production environment.

Note If a load balancer in front of VMware Identity Manager terminates SSL, the SSL certificate is applied to the load balancer.

Prerequisites

- Generate a Certificate Signing Request (CSR) and obtain a valid, signed SSL certificate from a CA. The certificate must be in the PEM format.
- For the Common Name part of the Subject DN, use the fully-qualified domain name that users use to access the VMware Identity Manager service. If the VMware Identity Manager appliance is behind a load balancer, this is the load balancer server name.
- If SSL is not terminated on the load balancer, the SSL certificate used by the service must include Subject Alternative Names (SANs) for each of the fully qualified domain names in the VMware Identity Manager cluster so that nodes within the cluster can make requests to each other. Also include a SAN for the FQDN host name that users use to access the VMware Identity Manager service, in addition to using it for the Common Name, because some browsers require it.

Procedure

1. In the VMware Identity Manager console, click the **Appliance Settings** tab.
2. Click **Manage Configuration** and enter the admin user password.
3. Select **Install SSL Certificates > Server Certificate**.
4. In the SSL Certificate field, select **Custom Certificate**.
5. In the **SSL Certificate Chain** text box, paste the server, intermediate, and root certificates, in that order.

   You must include the entire certificate chain in the correct order. For each certificate, copy everything between and including the lines -----BEGIN CERTIFICATE----- and -----END CERTIFICATE----.
6. In the **Private Key** text box, paste the private key. Copy everything between ----BEGIN RSA PRIVATE KEY and ---END RSA PRIVATE KEY.

7 Click **Add.**

Example: Certificate Examples

Certificate Chain Example
-----BEGIN CERTIFICATE-----
jlQvt9WdR9Vpg3WQT5+C3HU17bUOwvhp/r0+ ... W53+O05j5xsxzDJfWr1lqBlFF/OklYCPcyK1
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
WdR9Vpg3WQT5+C3HU17bUOwvhp/rjlQvt90+ ... O05j5xsxzDJfWr1lqBlFF/OklYCPW53+cyK1
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
dR9Vpg3WQTjlQvt9W5+C3HU17bUOwvhp/r0+ ... 5j5xsxzDJfWr1lqW53+O0BlFF/OklYCPcyK1
-----END CERTIFICATE-----

Private Key Example
-----BEGIN RSA PRIVATE KEY-----
jlQvtg3WQT5+C3HU17bU9WdR9VpOwvhp/r0+ ... 1lqBlFFW53+O05j5xsxzDJfWr/OklYCPcyK1
-----END RSA PRIVATE KEY-----

Installing Trusted Root Certificates

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

If the VMware Identity Manager server is configured behind a load balancer and SSL is terminated on the load balancer, install the load balancer's root certificate.

Procedure

1 In the VMware Identity Manager console, click the **Appliance Settings** tab.

2 Click **Manage Configuration** and enter the admin user password.

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

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

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

5 Click **Add.**

Installing a Passthrough Certificate

The **Passthrough Certificate** tab is used only when certificate authentication is configured on the embedded connector in a DMZ deployment scenario. It is not used in any other scenarios. See *Deploying VMware Identity Manager in the DMZ* for information.

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 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 VMware Identity Manager console.

Procedure

1 Log in to the VMware Identity Manager 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**.

Configure a 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, VMware Identity Manager 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 > Configure Syslog** 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.
- Ensure that VMware Identity Manager can reach the syslog server on port 514 (UDP).

Procedure

1 Log in to the VMware Identity Manager console.

2 Click the **Appliance Settings** tab, then 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.**

Results

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 logs directory.

Table 3-1. Log Files

Component	Location of Log File Linux	Location of Log File Windows	Description
Identity Manager Service Logs	`/opt/vmware/horizon/workspace/logs/horizon.log`	`<INSTALL_DIR>\opt\vmware\horizon\workspace\logs\horizon.log`	Information about activity on the service, such as entitlements, users, and groups.
Configurator Logs	`/opt/vmware/horizon/workspace/logs/configurator.log`	`<INSTALL_DIR>\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`	`<INSTALL_DIR>\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.
	`/opt/vmware/horizon/workspace/logs/connector-dir-sync.log`	*InstallDirectory*`\IDMConnector\opt\vmware\horizon\workspace\logs\connector-dir-sync.log`	Messages related to directory sync.
Update Logs	`/opt/vmware/var/log/update.log` `/opt/vmware/var/log/vami`	`<INSTALL_DIR>\opt\vmware\var\log\update.log`	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`	`<INSTALL_DIR>\opt\vmware\horizon\workspace\logs\catalina.log`	Apache Tomcat records of messages that are not recorded in other log files.

What to read next

- 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.

- Setting the VMware Identity Manager Service Log Level to DEBUG

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

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.

Collect the logs from each appliance in your environment.

Procedure

1. Log in to the VMware Identity Manager 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.

Setting the VMware Identity Manager Service Log Level to DEBUG

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

Procedure

1. Log in to the machine.
2. Change to the path to the `conf` directory.

   For Linux, go to `/usr/local/horizon/conf/`.

   For Windows, go to `\usr\local\horizon\conf\`.
3. Update the log level in the `cfg-log4j.properties`, `hc-log4j.properties`, and `saas-log4j.properties` files, which are the most commonly-used `log4j` files for the service.
   a. Edit the file.
   b. In the lines that have the log level set to `INFO`, replace `INFO` with `DEBUG`.

      For example, change:

      ```
      rootLogger.level=INFO
      ```

      to:

      ```
      rootLogger.level=DEBUG
      ```
   c. Save the file.

      A restart of the service or system is not required.

Manage Your Appliance Passwords

When you configured the VMware Identity Manager virtual appliance initially, you created passwords for the admin user. You can change admin password from the Appliance Settings tab in the VMware Identity Manager administration console.

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 VMware Identity Manager console, click the **Appliance Settings** tab.

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

3 To change the admin password, select **Change Password**.

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. For example, notification emails are sent when new local users are created, when a password is reset, or with the auto discovery verification token.

Procedure

1 Log in to the VMware Identity Manager console.

2 Click 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) If the SMTP server requires authentication, enter the user name and password.

6 Click **Save**.

7 To customize the sender's address in the email notifications, add the address to the `runtime-config.properties` file.

   a Log in to the VMware Identity Manager machine.

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

   ```
   notification.emails.support=emailaddress
   ```

   For example:

   ```
   notification.emails.support=admin@example.com
   ```

   c Save the file.

   d Restart the machine.

   ```
   service horizon-workspace restart
   ```

   This changes the sender's address from the default no-reply@vmwareidentity.com to the custom address.

Advanced Configuration for the VMware Identity Manager Appliance

4

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 for a typical deployment.

Read the following topics next:

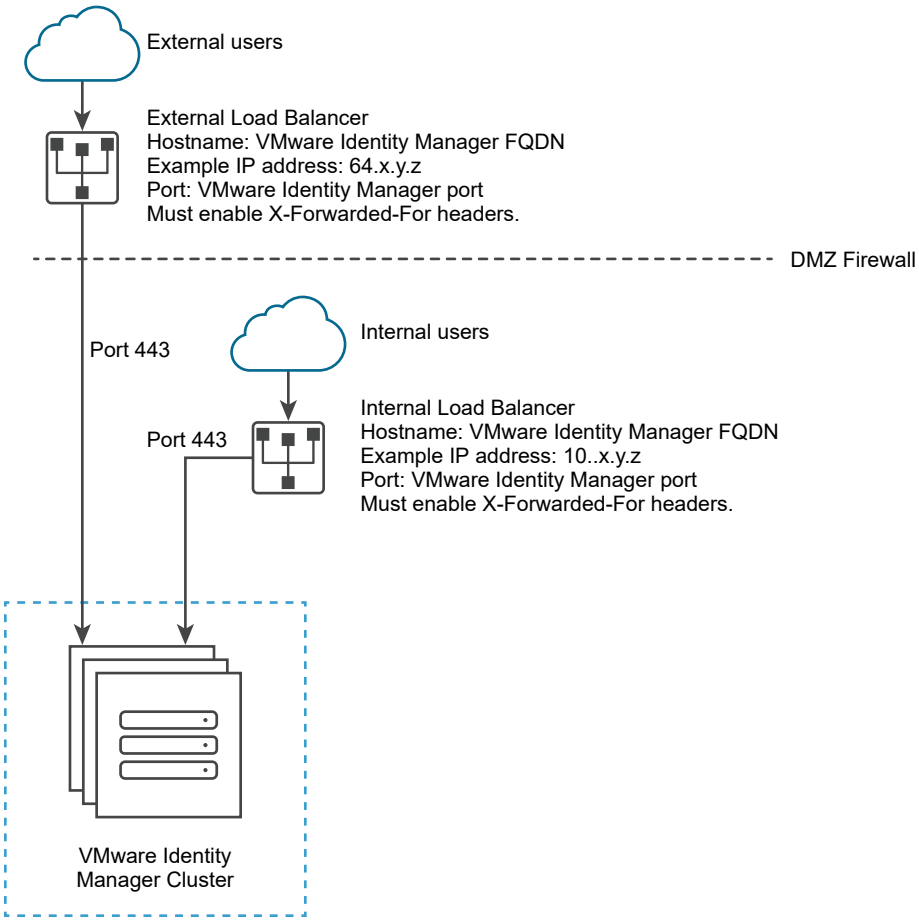
- Using a Load Balancer or Reverse Proxy to Enable External Access to VMware Identity Manager
- Configuring Failover and Redundancy in a Single Datacenter
- Deploying VMware Identity Manager in a Secondary Data Center for Failover and Redundancy
- Performing Disaster Recovery for VMware Identity Manager Using Site Recovery Manager

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

During deployment, the VMware Identity Manager machine 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 machines later. You might need to add more machines to provide redundancy and load balancing. The following diagram shows the basic deployment architecture that you can use to enable external access.

Figure 4-1. External Load Balancer Proxy with Virtual Machines



Specify VMware Identity Manager FQDN during Deployment

During the deployment of the VMware Identity Manager 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 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. Do not use 8443 as the port number, as this port number is the VMware identity Manager administrative port and is unique for each machine in a cluster.

Load Balancer Settings to Configure

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

- X-Forwarded-For Headers

You must enable X-Forwarded-For headers on your load balancer. VMware Identity Manager identifies the source IP address in the X-Forwarded-For headers and determines which authentication method to use based on the source IP address. 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 unavailable”.

- Enable Sticky Sessions

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

- WebSocket support

  The load balancer must have WebSocket support to enable secure communication channels between connectors and the VMware Identity Manager nodes.

- Ciphers with forward secrecy

  Apple iOS App Transport Security requirements apply to the Workspace ONE app on iOS. To enable users to use the Workspace ONE app on iOS, the load balancer must have ciphers with forward secrecy. The following ciphers meet this requirement:

  ECDHE_ECDSA_AES and ECDHE_RSA_AES in GCM or CBC mode

  as stated in the iOS 11 *iOS Security* document:

  "App Transport Security provides default connection requirements so that apps adhere to best practices for secure connections when using NSURLConnection, CFURL, or NSURLSession APIs. By default, App Transport Security limits cipher selection to include only suites that provide forward secrecy, specifically ECDHE_ECDSA_AES and ECDHE_RSA_AES in GCM or CBC mode."

Apply VMware Identity Manager Root Certificate to the Load Balancer

When the VMware Identity Manager virtual appliance is configured behind 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 root certificate can be downloaded from the **Appliance Settings > Manage Configuration > Install SSL Certificates > Server Certificate** page in the VMware Identity Manager administration console.

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.

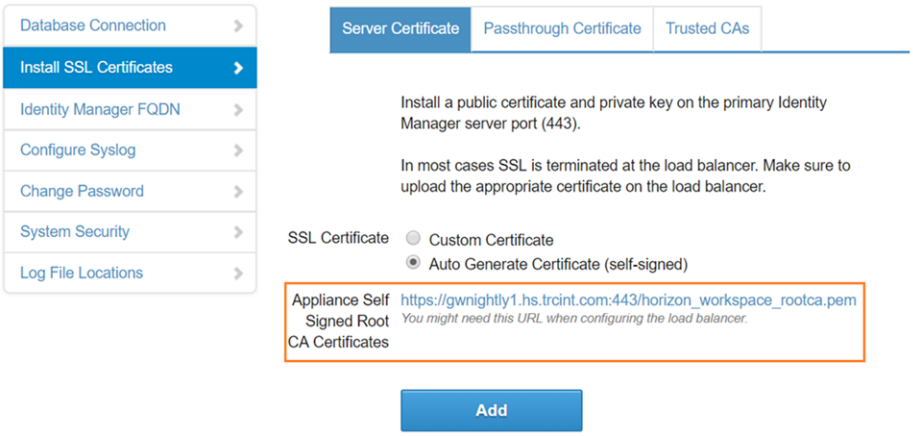
Procedure

1 In the VMware Identity Manager console, select the **Appliance Settings** tab, then click **VA Configuration > Manage Configuration**.

2 In the dialog box that appears, enter the admin user password.

3 Select **Install SSL Certificates > Server Certificate**.

4 Click the **Appliance Self Signed Root CA Certificates** link.



The certificate is displayed.

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 Manager appliance.

Apply Load Balancer Root Certificate to VMware Identity Manager

When the VMware Identity Manager virtual appliance is configured behind 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

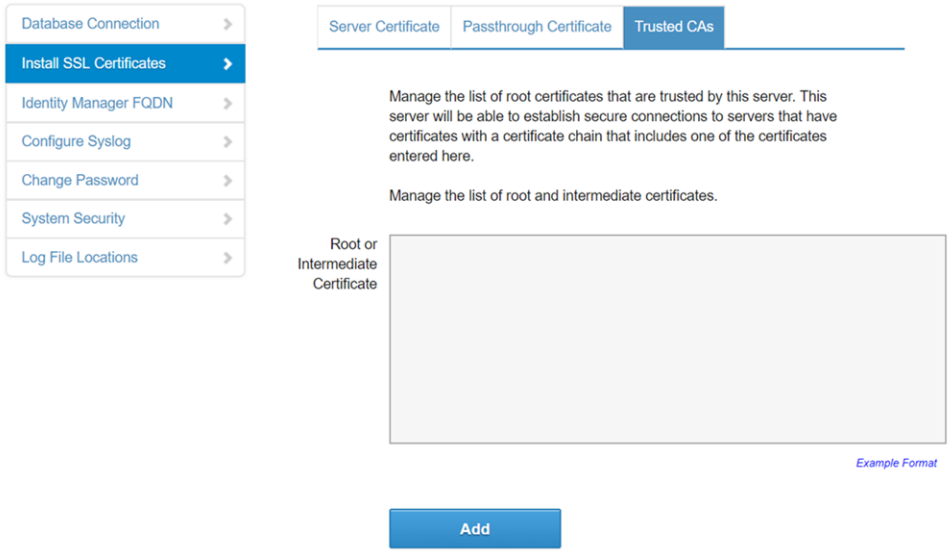
1 Obtain the load balancer root certificate.

2 In the VMware Identity Manager console, select the **Appliance Settings** tab, then click **VA Configuration > Manage Configuration**.

3 In the dialog box that appears, enter the admin user password.

4 Select **Install SSL Certificates > Trusted CAs**.

5 Paste the load balancer root certificate into the **Root or Intermediate Certificate** text box.



6 Click **Add**.

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.

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
```

Results

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 appliances shuts down for any reason, VMware Identity Manager is still available.

To create the cluster, 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.

Note It is suggested to use the "Add Components (Scale out)" option in VMware Aria Suite Lifecycle when VMware Identity Manager is integrated with VMware Aria Suite Lifecycle.

Refer to Scale out Workspace ONE Access for high availability in VMware Aria Suite Lifecycleto know more about Scale out option.

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.

What to read next

Procedure

1. Recommendations for VMware Identity Manager Cluster

   Follow these guidelines for setting up a VMware Identity Manager cluster.
2. Change VMware Identity Manager FQDN to Load Balancer FQDN
3. Clone the Virtual Appliance

4 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.

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

6 Removing a Node from a Cluster

   If a node in the VMware Identity Manager cluster is not functioning correctly and you are unable to recover it, you can remove it from the cluster with the Remove Node command. The command removes the node entries from the VMware Identity Manager database.

Recommendations for VMware Identity Manager Cluster

Follow these guidelines for setting up a VMware Identity Manager cluster.

Recommended Number of Nodes in VMware Identity Manager Cluster

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

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.

Network Partitions

Creating a network partition between nodes in a VMware Identity Manager cluster is not recommended. If a network partition exists between VMware Identity Manager service nodes such that the nodes cannot communicate with each other, and if all the nodes are still accessible from the load balancer, letting login requests go to any of the partitioned nodes, you might encounter the following problems:

- You might see stale data across requests. For example, changes made to an access policy on one node might not apply to login requests that go to another node if there is a partition between the nodes.
- Login calls that use the outbound connector might fail.

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

Procedure

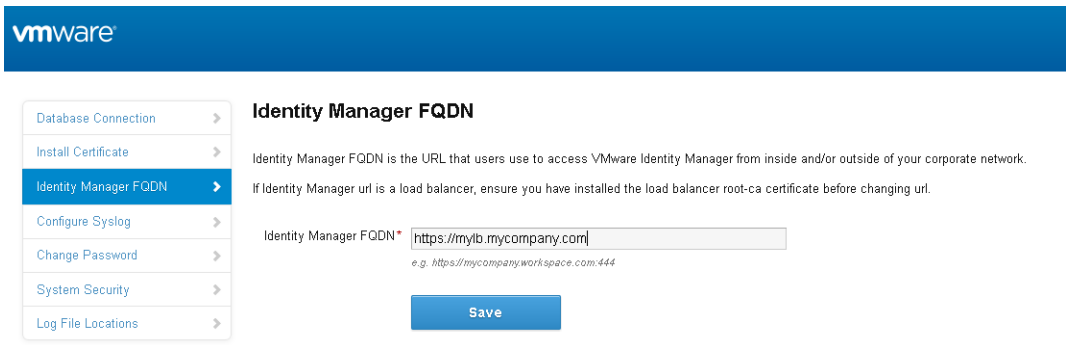
1. Log in to the VMware Identity Manager administration console.
2. Select the **Appliance Settings** tab.
3. In the Virtual Appliance Configuration page, click **Manage Configuration**.
4. Enter your administrator password to log in.
5. Click **Identity Manager Configuration**.
6. In the **Identity 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.example.com`

   to the following:

   `https://mylb.example.com`



7 Click **Save**.

Results

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

Note When Scale Out or Add Components on VMware Aria Suite Lifecycle option is used, VMware Aria Suite Lifecycle will update FQDN information and it is not required to do it manually. Refer Scale out Workspace ONE Access for high availability in VMware Aria Suite Lifecycle for more details.

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 reduce 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 Create the VMware Identity Manager Service Database.
- 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**.

Results

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 cluster is created before adding the cloned virtual appliance to the load balancer.

  Elasticsearch, a search and analytics engine, is 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.

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

  a Log in to the VMware Identity Manager 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 *Directory Integration with VMware Identity Manager*.

- For directories of type Active Directory over 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 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.

- 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.

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

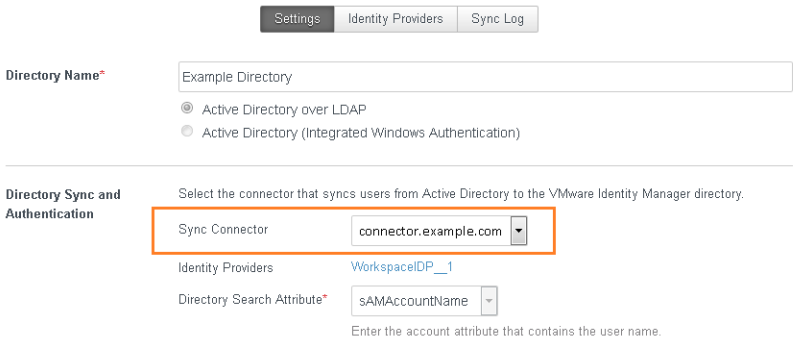
1 Log in to the VMware Identity Manager console.

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**.

Removing a Node from a Cluster

If a node in the VMware Identity Manager cluster is not functioning correctly and you are unable to recover it, you can remove it from the cluster with the Remove Node command. The command removes the node entries from the VMware Identity Manager database.

You can check the health of the nodes in your cluster by viewing their status in the System Diagnostics Dashboard. A `The current node is in a bad state` message indicates that the node is not functioning correctly.

Important Use the Remove Node command sparingly. Only use it when a node is in an unrecoverable state and must be removed completely from the VMware Identity Manager deployment.

Note You cannot use the Remove Node command to remove the last node in a cluster.

Remove the Node from the Cluster

After you disassociate the connector component of the node from domains, directory sync settings, and the Built-in identity provider, you can remove the node from the cluster.

Note You cannot use the Remove command to remove the last node in a cluster.

Prerequisites

- To remove a node, you must log in as a tenant administrator, that is, a local administrator on the VMware Identity Manager service. A domain administrator synced from the enterprise directory does not have the necessary permissions.
- You have disassociated the node's connector component from domains, directory sync settings, and the Built-in identity provider, if necessary. See #unique_52.

Procedure

1. Shut down the node virtual machine.
   a. Log in to the vCenter Server instance.
   b. Right-click the node virtual machine and select **Power > Power Off**.
2. Remove the node from the load balancer.
3. In the VMware Identity Manager console, remove the node.
   a. Log in to the VMware Identity Manager console as a local administrator.
   b. Click the down arrow on the **Dashboard** tab and select **System Diagnostics Dashboard**.

c Locate the node you want to remove.

The node displays the following status:

```
The current node is in a bad state. Do you want to want to remove it?
```

d Click the **Remove** link that is displayed next to the message.

Results

The node is removed from the cluster. Entries for the node are removed from the VMware Identity Manager database. The node is also removed from the embedded Elasticsearch and Ehcache clusters.

What to do next

Wait 5-15 minutes for the embedded Elasticsearch and Ehcache clusters to stabilize before using any other commands.

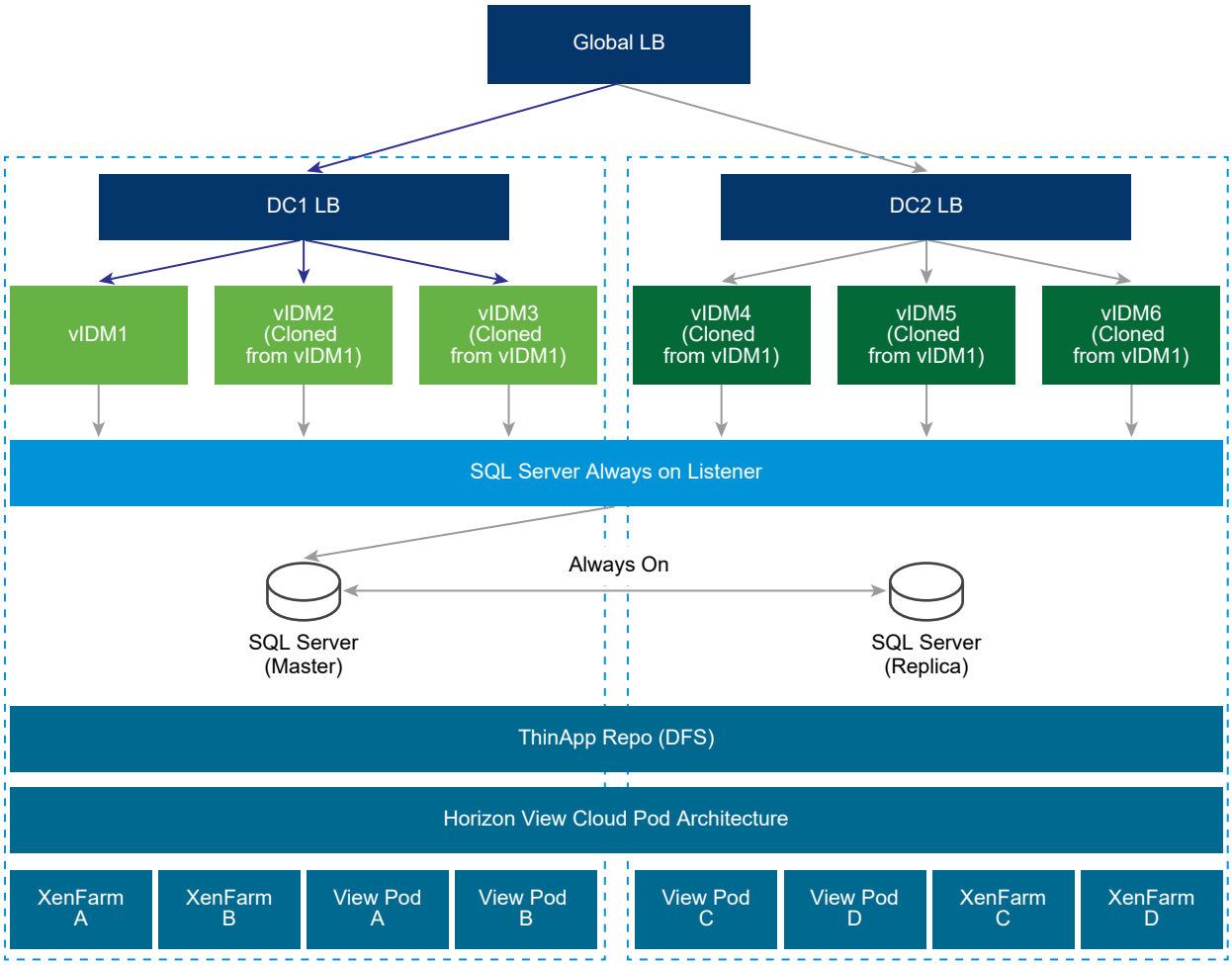
Deploying VMware Identity Manager in a Secondary Data Center for Failover and Redundancy

To provide failover capabilities if the primary VMware Identity Manager data center becomes unavailable, you must deploy VMware Identity Manager in a secondary data center.

For disaster recovery, the recommendation is to use VMware Site Recovery Manager. See Performing Disaster Recovery for VMware Identity Manager Using Site Recovery Manager. If you do not meet the requirements for Site Recovery Manager, implement the following approach.

By using a secondary data center, end users can log in and use applications with minimal downtime. Also, with a secondary data center, you can upgrade VMware Identity Manager to the next version with minimal downtime. See Upgrading VMware Identity Manager with Minimal Downtime.

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



Follow these guidelines for a multiple data center deployment.

- Cluster Deployment: You must deploy a set of VMware Identity Manager virtual appliances in two separate data centers.
  - A set of three or more VMware Identity Manager virtual appliances as one cluster in one data center.
  - Another set of three or more VMware Identity Manager virtual appliances as another cluster in a second data center.

  See Setting up a Secondary Data Center for more information.
- Database: VMware Identity Manager uses the database to store data. For a multiple data center 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 preferable. See Overview of Always On Availability Groups (SQL Server) on the Microsoft website for information. VMware Identity Manager functionalities are designed for minimal latency between the database and the VMware Identity Manager appliance. Therefore, appliances in one data center are designed 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 failover to that data center, most admin operations, like adding users or applications, or entitling users, will not work.
- Fail-Back to Primary: In most failure scenarios, you can fail back to the primary data center after that data center is back to normal. See Failback to Primary Data Center for information.
- Promote Secondary to Primary: If an extended data center failure occurs, the secondary data center can be promoted to primary. See Promoting Secondary Data Center to Primary Data Center for information.
- Fully Qualified Domain Name: The fully qualified domain name to access VMware Identity Manager must 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. Create separate Elasticsearch clusters in each data center. See Setting up a Secondary Data Center for more information.
- Active Directory: VMware Identity Manager can connect to Active Directory using the LDAP API or using Integrated Windows Authentication. With both of these methods, VMware Identity Manager can use 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. Delivering these resources from a data center that is closer to the user, also called Geo-Affinity, is important. 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 multiple data center 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 run Horizon View resources from the View pods configured in the secondary data center. See Configure Failover Order of Horizon View and Citrix-published Resources 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 run Citrix resources from the XenFarms configured in the secondary data center. See Configure Failover Order of Horizon View and Citrix-published Resources 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

Requirements

Ensure that you meet these requirements for deploying VMware Identity Manager in a secondary data center.

- Ensure that the VMware Identity Manager certificate includes the FQDN of the load balancer from the primary data center as well as the FQDN of the load balancer from the secondary data center. Otherwise, the certificate must be a wildcard certificate.
- Ports 443 and 8443 must be open between all VMware Identity Manager instances, both within a cluster and across clusters in different data centers.

Modify the Primary Data Center for Replication

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

Elasticsearch, a search and analytics engine embedded in the VMware Identity Manager virtual appliance, is used for auditing, reports, and directory sync logs.

Make 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. Add the load balancer FQDN of the secondary data center cluster to the `/usr/local/horizon/conf/runtime-config.properties` file of each node in the primary data center cluster.
   a. Edit the `/usr/local/horizon/conf/runtime-config.properties` file.

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

   b. Add this line to the file:

      ```
      analytics.replication.peers=https://LB_FQDN_of_second_cluster
      ```

2. Restart the VMware Identity Manager service on all the nodes.

   ```
   service horizon-workspace restart
   ```

3. Verify that the cluster is set up correctly by running the following command on all the nodes in the cluster.

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

   The command, which verifies Elasticsearch health, 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
   }
   ```

What to do next

Verify that the cluster in the primary data center is set up correctly by viewing the Systems Diagnostics dashboard.

Verify Cluster in Primary Data Center

Before you set up the secondary data center, verify that the cluster in the primary data center is set up correctly. Also verify that the embedded components Elasticsearch and Ehcache are clustered correctly.

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

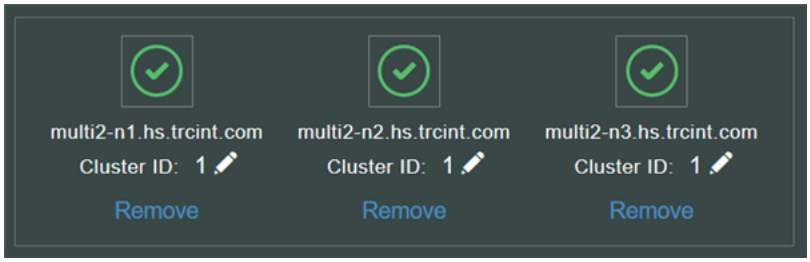
Prerequisites

You set up a VMware Identity Manager cluster in the primary data center and configured the nodes for Elasticsearch replication.

Procedure

1 In the VMware Identity Manager console, select the **Dashboard > System Diagnostics Dashboard** tab.

2 On the top panel, locate the cluster information.



3 Verify that the instances are grouped correctly by checking the Cluster IDs of the instances, and make changes if necessary.

All instances in a cluster must have the same Cluster ID.

- To update the **Cluster ID** of an instance, click the pencil icon next to the number.
- To remove an instance from the cluster, click **Remove**.

4 For each instance listed in the left pane, scroll down to the **Integrated Components** section and verify that the Elasticsearch and Ehcache cluster information is correct.

For example:

Integrated Components

Database Connection: Connection test successful.
Audit enabled.: yes
Audit Worker Thread Alive: yes
Audit Queue Size: 3
Audit Poll Interval: 1000
Analytics Connection: Connection test successful.
Messaging Connection: Connection test successful.
EhCache Cluster Peers: multi2-n2.hs.trcint.com, multi2-n3.hs.trcint.com
EhCache Cluster Diagnostics: Working
Elasticsearch - Health: green
Elasticsearch - master node: 10.143.xx.xx
Elasticsearch - indices count: 7
Elasticsearch - docs count: 217626
Elasticsearch - unassigned shards: 0
Elasticsearch - cluster nodes count: 3
Elasticsearch - cluster nodes list: 10.143.xx.xx, 10.143.xx.xx, 10.143.xx
RabbitMQ - node name: rabbit@win-upg-n1
RabbitMQ - number of queues: 32
RabbitMQ - status: ok

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.

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.

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 for Elasticsearch replication.

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

Procedure

1. Add the load balancer FQDN of the primary data center cluster to the `/usr/local/horizon/conf/runtime-config.properties` file of each node in the secondary data center cluster.
   a. Edit the `/usr/local/horizon/conf/runtime-config.properties` file.

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

   b. Add this line to the file:

      ```
      analytics.replication.peers=https://LB_FQDN_of_primary_cluster
      ```

2. Restart the VMware Identity Manager service on all the nodes.

   ```
   service horizon-workspace restart
   ```

3. Verify that the cluster is set up correctly by running the following command on all the nodes in the cluster.

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

   The command, which verifies Elasticsearch health, 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
   }
   ```

Set Cluster ID and Verify Cluster in Secondary Data Center

After you create nodes in the secondary data center and configure Elasticsearch for replication, set the Cluster ID for the secondary data center and verify that the cluster is set up correctly.

Procedure

1 In the VMware Identity Manager console, select the **Dashboard > System Diagnostics Dashboard** tab.

2 On the top panel, change the **Cluster ID** of all the nodes in the secondary data center cluster to a different number than the first data center.

For example:

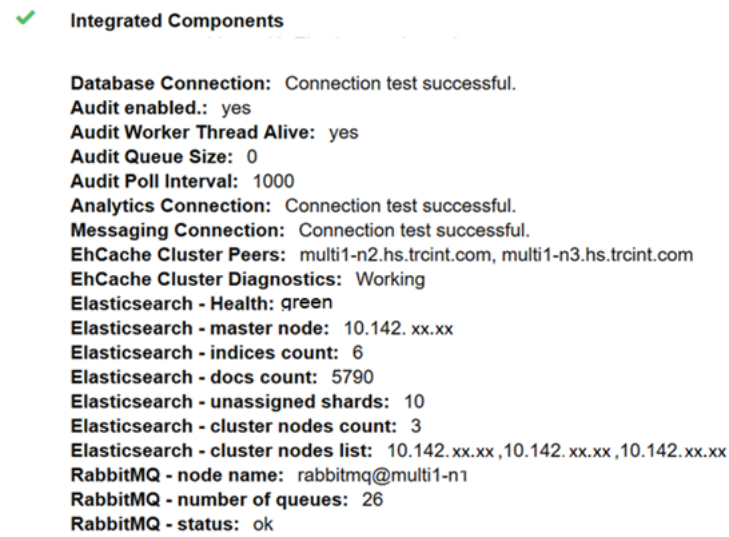
3 Verify that the nodes are grouped correctly by checking the Cluster IDs of the nodes, and make changes if necessary.

All nodes in a cluster must have the same Cluster ID.

- To update the **Cluster ID** of a node, click the pencil icon next to the number.
- To remove a node from the cluster, click **Remove**.

4 For each node listed in the left pane, scroll down to the **Integrated Components** section and verify that the Elasticsearch and Ehcache cluster information is correct.

For example:



Edit runtime-config.properties File in Secondary Data Center to Set Read-Only Mode

You must edit the `runtime-config.properties` files for the VMware Identity Manager appliances in the secondary data center to configure the appliances for read-only access. Also change the JDBC URL on the secondary data center nodes if you are not using technologies such as SQL Server Always On.

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.
3. Configure the VMware Identity Manager appliance to have read-only access by adding the following line:

   ```
   read.only.service=true
   ```

4. Also add the following line to the file:

   ```
   cache.service.type=ehcache
   ```

   Note `cache.service.type=ehcache` is required if you set `read.only.service=true`. If `read.only.service=false`, then the default is `cache.service.type=rds`.

5. Save the file.
6. Change the JDBC URL on the secondary data center nodes if you are not using technologies such as SQL Server Always On.

   See Configure VMware Identity Manager to Use an External Database for information.

7. Restart the Tomcat server on the appliance.

   ```
   service horizon-workspace restart
   ```

Configure Failover Order of Horizon View and Citrix-published Resources

For Horizon View and Citrix-published 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` command in both data centers to set up the failover order.

Note This procedure does not apply to environments using Horizon View Cloud Pod Architecture (CPA).

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 Horizon pods or Citrix 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 Horizon and Citrix configuration pages in the VMware Identity Manager console.

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 service instances, type:

```
hznAdminTool -j clusterInstances
```

A list of service instances is displayed. The `"id"` value is the service instance ID. For example:

```
{
"clusterInstances":[{
"version" : "3.2.0.1 Build 8223322",
"uuid" : "7451fe26-5b02-32ef-bfe6-6fe0a8710a14",
"status" : "Active",
"lastUpdated" : 1523372105701,
"hostname" : "server.example.com",
"datacenterId" : 0,
"id" : 2,
"ipaddress" : "10.143.xxx.xx"}
]}
```

3 For each service instance in your organization, configure the failover order for Horizon and Citrix-based resources with the folllowing command:

```
hznAdminTool failoverConfiguration -configType <configType> -configuration
<configuration> -serviceInstanceId <serviceInstanceId>
```

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 Horizon Connection Server host names that are listed in the Horizon View configuration page in the VMware Identity Manager 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":`

For example:

```
hznAdminTool failoverConfiguration -configType VIEW -configuration
pod1vcs1.domain.com,pod2vcs1.hs.trcint.com -serviceInstanceId 1
```

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

Results

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 Horizon View and Citrix-published resources, run the command:

```
hznAdminTool failoverConfigurationList -configType <configtype>
```

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

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

Clear Cache in Secondary Data Center

After you finish setting up the primary and secondary data centers, clear the caches in the secondary data center. This is in preparation for a failover. When you fail over to the secondary data center, caches in the secondary data center should be empty.

Use the REST API described here to clear the caches. Another way to clear cache is to reboot the virtual appliances.

Procedure

- Run the following REST API from a REST client such as Postman.

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

  Method: POST

  Add Headers:

  ```
  Authorization: HZN <cookie_value>
  Accept: application/vnd.vmware.horizon.manager.cache.removal.response+json
  Content-type: application/vnd.vmware.horizon.manager.cache.removal.request+json’
  ```

Add in Body (raw) section:

```
{
"cacheNames":[]
}
```

Note

- You must run the API as the tenant administrator, that is, the administrator created in the System domain when you install VMware Identity Manager. Domain accounts synced from your enterprise directory cannot perform this function.
- You can obtain the `HZN` cookie by logging into the VMware Identity Manager service as the tenant administrator, then accessing your browser's cookie cache.
- Empty `cacheNames` indicates remove all caches.

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:jtds:sqlserver://<hostname_or_IP_address:port#>/
<saasdb>;integratedSecurity=true;domain=<domainname>;useNTLMv2=true;multiSubnetFailover=true
```

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.

See Using a DNS Record to Control Which Data Center is Active.

The VMware Identity Manager appliances in the secondary data center are in read-only mode. Therefore, most administrator operations, such as adding users or apps, or entitling users, are not available. See VMware Identity Manager Activities Not Available in Read-Only Mode.

Important After you fail over to the secondary data center, you must clear all caches on the original primary data center. In case you need to fail over to the original primary data center, caches in that data center should be empty.

You can use a REST API to clear the cache. Run the following REST API from a REST client such as Postman:

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

Method: POST

Add Headers:

```
Authorization: HZN <cookie_value>
Accept: application/vnd.vmware.horizon.manager.cache.removal.response+json
Content-type: application/vnd.vmware.horizon.manager.cache.removal.request+json'
```

Add in Body (raw) section:

```
{
"cacheNames":[]
}
```

Note

- You must run the API as the tenant administrator, that is, the administrator created in the System domain when you install VMware Identity Manager. Domain accounts synced from your enterprise directory cannot perform this function.
- You can obtain the `HZN` cookie by logging into the VMware Identity Manager service as the tenant administrator, then accessing your browser's cookie cache.
- Empty `cacheNames` indicates remove all caches.

Another way to clear cache is to reboot the virtual appliances.

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 the primary data center.

Mobile SSO for iOS Authentication

If you are using Mobile SSO for iOS authentication, update both the A and AAAA DNS entries to point to the load balancer in the secondary data center. For example:

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

Note If you are using the hybrid KDC feature, this is not required.

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 Horizon 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 Horizon 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. Some activities in the VMware Identity Manager 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 Console Read-Only Mode

The following are some of the limitations in the VMware Identity Manager 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 Horizon, XenApp, and other resources

- Editing 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 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 Bookmarks page
- Change their password from their 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.

2. Clear the cache in the secondary data center.

   Run the following REST API from a REST client such as Postman:

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

   Method: POST

   Add Headers:

   ```
   Authorization: HZN <cookie_value>
   Accept: application/vnd.vmware.horizon.manager.cache.removal.response+json
   Content-type: application/vnd.vmware.horizon.manager.cache.removal.request+json'
   ```

Add in Body (raw) section:

```
{
"cacheNames":[]
}
```

Note

- You must run the API as the tenant administrator, that is, the administrator created in the System domain when you install VMware Identity Manager. Domain accounts synced from your enterprise directory cannot perform this function.
- You can obtain the `HZN` cookie by logging into the VMware Identity Manager service as the tenant administrator, then accessing your browser's cookie cache.
- Empty `cacheNames` indicates remove all caches.

Another way to clear cache is to reboot the virtual appliances.

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.

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. Change the `cache.service.type=ehcache` line to `cache.service.type=rds`.
5. Save the `runtime-config.properties` file.
6. Restart the Tomcat server on the appliance.

   ```
   service horizon-workspace restart
   ```

Upgrading VMware Identity Manager with Minimal Downtime

With a multi-data center deployment, you can upgrade VMware Identity Manager to the next version with minimal 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 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.

Performing Disaster Recovery for VMware Identity Manager Using Site Recovery Manager

The information that follows describes how to use VMware Site Recovery Manager™ with other VMware products to configure a disaster-recovery solution for VMware Identity Manager in an on-premises environment.

About Disaster Recovery for VMware Identity Manager

A disaster-recovery deployment requires a protected site and a recovery site. The recommended approach to setting up disaster recovery for VMware Identity Manager is to leverage Site Recovery Manager.

Site Recovery Manager is a disaster-recovery automation software application that provides policy-based management, non-disruptive testing, and automated orchestration.

To protect your VMware Identity Manager deployment, Site Recovery Manager automates every aspect of running a disaster recovery plan to expedite the recovery process and eliminate the risks involved in using a manual process.

The Amount of Downtime to Expect

Site Recovery Manager allows VMware Identity Manager to operate from the recovery site. If a failover occurs, the Recovery Time Objective (RTO) depends on several factors, such as network bandwidth across sites, Site Recovery Manager architecture, and the replication strategy you deploy. To estimate the amount of downtime, consider details such as how long virtual machines and services take to start. These factors combined define the RTO.

See Additional VMware Documentation

Much of the information that follows about using Site Recovery Manager to configure a disaster-recovery solution for VMware Identity Manager points to other VMware documentation, such as the VMware Site Recovery Manager documentation.

For information about how to install and configure Site Recovery Manager and the different technologies, such as the replication technologies, see *VMware Site Recovery Manager Installation and Configuration*, *VMware Site Recovery Manager Administration* and, if you are using VMware vSphere Replication, *VMware vSphere Replication Administration*.

Overview of VMware Site Recovery Manager

VMware Site Recovery Manager is a business continuity and disaster recovery solution that helps you to plan, test, and run the recovery of virtual machines between a protected vCenter Server site and a recovery vCenter Server site.

You can configure Site Recovery Manager to protect virtual machines in different ways.

Datastore groups

Protect the virtual machines in datastore groups by using third-party disk replication mechanisms to configure array-based replication. Array-based replication surfaces replicated datastores to recover virtual machine workloads.

Individual virtual machines

Protect the individual virtual machines on a host by using Site Recovery Manager in combination with VMware vSphere Replication.

Storage policies

Protect virtual machines based on their association with specific storage policies. Protecting virtual machines by using storage policies requires array-based replication.

You can use Site Recovery Manager to implement different types of recovery from the protected site to the recovery site.

Planned migration

The orderly evacuation of virtual machines from the protected site to the recovery site. Planned migration prevents data loss when migrating workloads in an orderly fashion. For planned migration to succeed, both sites must be running and fully functioning.

Disaster recovery

Similar to planned migration except that disaster recovery does not require that both sites be up and running, for example if the protected site goes offline unexpectedly. During a disaster recovery operation, failure of operations on the protected site is reported but is otherwise ignored.

Site Recovery Manager orchestrates the recovery process with the replication mechanisms, to minimize data loss and system down time.

- At the protected site, Site Recovery Manager shuts down virtual machines cleanly and synchronizes storage, if the protected site is still running.
- Site Recovery Manager powers on the replicated virtual machines at the recovery site according to a recovery plan.

A recovery plan specifies the order in which virtual machines start up on the recovery site. A recovery plan specifies network parameters, such as IP addresses, and can contain user-specified scripts that Site Recovery Manager can run to perform custom recovery actions on virtual machines.

Site Recovery Manager lets you test recovery plans. You conduct tests by using a temporary copy of the replicated data in a way that does not disrupt ongoing operations at either site.

Configuring and Using Site Recovery Manager for VMware Identity Manager

You must configure Site Recovery Manager to protect your VMware Identity Manager deployment. Secure this protection by properly installing and configuring Site Recovery Manager.

Prepare the Environment

Before you configure Site Recovery Manager, set up the proper environment.

Confirm that your deployment meets the following prerequisites at each site.

- Configure ESXi 6.7 u2 or later on the protected and recovery sites.
- Update VMware Tools to the latest version.
- Install Site Recovery Manager 8.1 or later on each ESXi host.

  For Site Recovery Manager installation instructions, see the respective version of *Site Recovery Manager Installation and Configuration*.
- Verify that the protected and recovery sites are connected over the same VLAN, Layer 2 over Layer 3, or stretched VLAN.
- For VMware Identity Manager 19.03 only, perform the steps in the following VMware Knowledge Base article, https://kb.vmware.com/s/article/74709, to improve Elasticsearch full cluster restart.
- Verify that you have successfully deployed VMware Identity Manager on the protected site.

Table 4-1. Disaster Recovery Components Per Site

Site A - Protected	Site B - Recovery
vCenter Server 1	vCenter Server 2
vSphere Replication 1 or array-based replication 1	vSphere Replication 2 or array-based replication 2
Site Recovery Manager 1	Site Recovery Manager 2

Configure VMware Identity Manager at Each Site

Install and configure VMware Identity Manager. To provide high availability within the data center, use multiple VMware Identity Manager service nodes. Three service nodes is a common deployment. However, you can configure a single service node for small, non-mission critical deployments. You deploy the components at the protected site and replicate the deployment to the recovery site.

The following example is of a deployment with three-service nodes, two external connectors, and an external database.

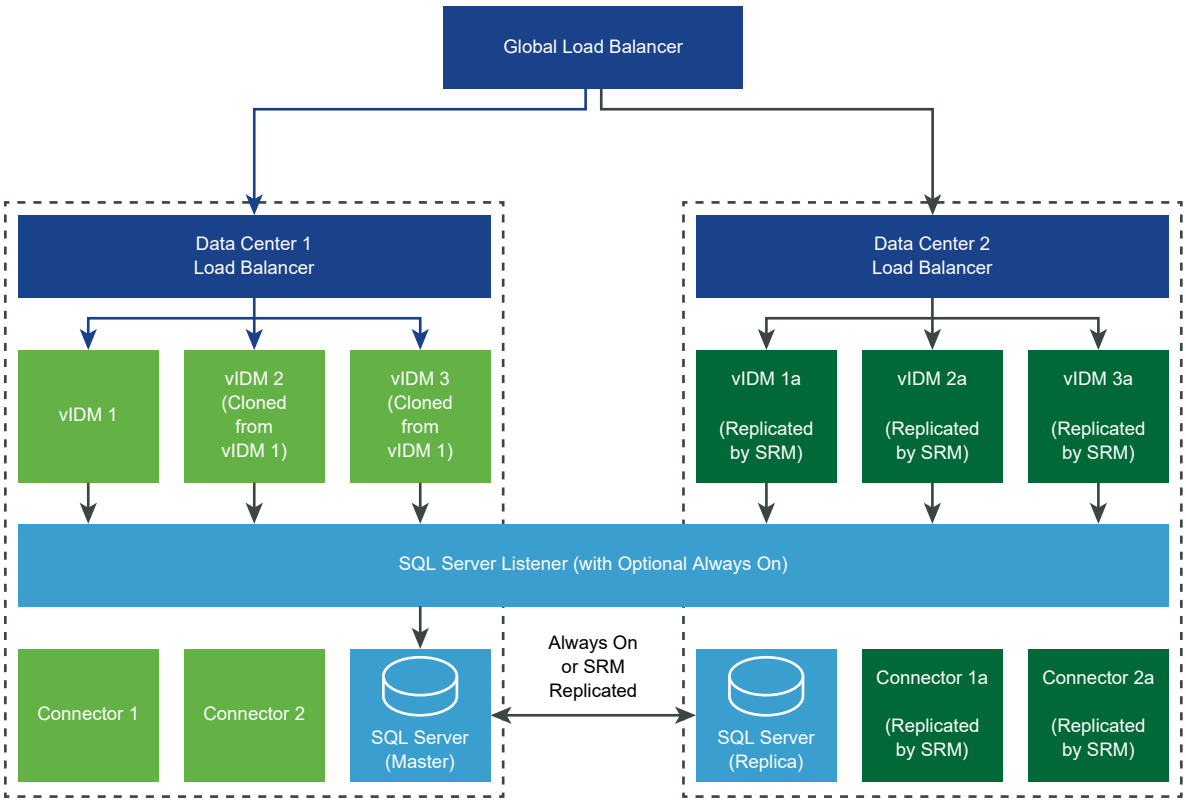


Table 4-2. Typical VMware Identity Manager Cluster Deployment at Protected Site

Site A - Protected Site VMware Identity Manager Deployment
External Database
Service Node 1

Table 4-2. Typical VMware Identity Manager Cluster Deployment at Protected Site (continued)

Site A - Protected Site VMware Identity Manager Deployment
Service Node 2
Service Node 3
Connector 1
Connector 2

If you are using the SQL Server Always On capability, you do not need to protect SQL using Site Recovery Manager, which reduces the Site Recovery Manager protection groups to only VMware Identity Manager virtual machines.

Key tasks you must perform to configure and use Site Recovery Manager for VMware Identity Manager include the following.

- Configure a replication-technology type, vSphere Replication or array-based replication. See the appropriate documentation, such as *Site Recovery Manager Administration* and, if you use vSphere Replication, also see *VMware vSphere Replication Administration*.
- Create protection groups. See the appropriate documentation, such as *Site Recovery Manager Administration*, specifically information about creating and managing protection groups based on the replication technology type you use.
- Create and edit a recovery plan. See both the *Site Recovery Manager Administration* guide and the topics that follow in this guide about creating and editing a recovery plan.
- Test and Run a Recovery Plan. See both the Test and Run a Recovery Plan topic and the *Site Recovery Manager Administration* guide.
- Perform a Failback. See both the Perform a Failback After a Disaster Recovery or Planned Migration topic and the *Site Recovery Manager Administration* guide.

Adjust the recovery.powerOnDelay Setting

When you create a recovery plan in Site Recovery Manager, adjust the **recovery.powerOnDelay** setting.

Adjusting the **recovery.powerOnDelay** setting in Site Recovery Manager can improve the VMware Identity Manager disaster-recovery experience. After Site Recovery Manager recovers a virtual machine, a certain amount of time is required for post power-on steps to run and for dependent virtual machines to start. Adding **120** seconds of delay can provide the virtual machine with the amount of process time required.

Perform this specific configuration when you create a recovery plan in Site Recovery Manager. The following instructions are for 8.2, but might also be applicable to other versions. See *Site Recovery Manager Administration*.

Procedure

1 In the vSphere Client or the vSphere Web Client, click **Site Recovery > Open Site Recovery**.

2 On the **Site Recovery** home tab, select a site pair, and click **View Details**.

3 In the left pane, click **Configure > Advanced Settings > Recovery**.

4 Select a site and click **Edit**.

5 In the **recovery.powerOnDelay** text box, enter **120**.

6 Click **OK**.

Specify the Recovery Priority of Each VMware Identity Manager Virtual Machine

When you create a recovery plan in Site Recovery Manager, assign the proper priority to each virtual machine in the VMware Identity Manager deployment.

Perform this specific configuration when you create a recovery plan in Site Recovery Manager. The following instructions are for 8.2, but might also be applicable to other versions. See *Site Recovery Manager Administration*.

The following example illustrates how you can prioritize the virtual machines in a VMware Identity Manager cluster deployment.

Component	Priority Setting
External database	**1**
All service nodes	**2**
All connector nodes	**3**

Procedure

1 In the vSphere Client or the vSphere Web Client, click **Site Recovery > Open Site Recovery**.

2 On the **Site Recovery** home tab, select a site pair, and click **View Details**.

3 Click the **Recovery Plans** tab, click a recovery plan, and click **Virtual Machines**.

4 Right-click a virtual machine and click **Priority Group**.

5 Select a new priority for the virtual machine.

The highest priority is **1**. The lowest priority is **5**.

6 To confirm the change of priority, click **Yes**.

Configure Virtual Machine Dependencies

Configure a dependency for each VMware Identity Manager service node virtual machine on a respective external database.

Perform this specific configuration when you create a recovery plan in Site Recovery Manager. The following instructions are for 8.2, but might also be applicable to other versions. See *Site Recovery Manager Administration*.

When a recovery plan runs, Site Recovery Manager starts the virtual machines that other virtual machines depend on before it starts the virtual machines with the dependencies.

You can configure dependencies for many reasons. A common dependency for VMware Identity Manager is the dependency of a VMware Identity Manager service node on an external database. The following dependencies apply.

Component	Virtual Machine Dependencies
External Database	Not Applicable
All service nodes	External Database
All connector nodes	All Service Nodes

Procedure

1 In the vSphere Client or the vSphere Web Client, click **Site Recovery > Open Site Recovery**.

2 On the **Site Recovery** home tab, select a site pair, and click **View Details**.

3 Click the **Recovery Plans** tab, click a recovery plan, and click **Virtual Machines**

4 Right-click a virtual machine that depends on one or more other virtual machines and click **Configure Recovery**.

5 Expand **VM Dependencies**.

6 From the drop-down menu, select **View all**.

7 Select one or more virtual machines from the list of all virtual machines in the selected recovery plan.

The selected virtual machines are added to the list of dependencies.

8 Verify that the virtual machines in the **VM Dependencies** list are on and verify that the status of the dependencies is **OK**.

9 (Optional) To remove a dependency, select **View VM Dependencies** from the drop-down menu, select a virtual machine from the list of virtual machines that this virtual machine depends on, and click **Remove**.

10 Click **OK**.

Enable Network Compression for vSphere Replication Data

If you deploy vSphere Replication as your replication-technology type, enable network compression for the vSphere Replication data.

Configure this specific setting when you configure vSphere Replication with Site Recovery Manager. The following instructions are for 8.2, but might also be applicable to other versions. See *Site Recovery Manager Administration* and *VMware vSphere Replication Administration*.

Enabling network compression speeds up the replication process across vCenter Server instances.

Procedure

- To enable network compression, when you configure vSphere Replication, select the **Enable network compression for VR data** check box.

Test and Run a Recovery Plan

To run a recovery plan or planned migration of your VMware Identity Manager deployment as smoothly as possible, first test the plan to verify that the virtual machines in the VMware Identity Manager deployment recover as expected to the recovery site. After successful tests and requisite cleanup operations, run a recovery plan as necessary for a planned migration or disaster recovery.

You perform a test run of a recovery plan on a test network and on a temporary snapshot of replicated data at the recovery site. The test does not have a permanent effect on the protected or recovery site.

You perform an actual run of a recovery plan on the production deployment of VMware Identity Manager, which significantly affects both sites.

Prerequisites

Configure Site Recovery Manager to protect your VMware Identity Manager deployment. The configuration includes the creation of a recovery plan.

Procedure

- Follow the instructions provided in *Site Recovery Manager Administration* about testing and running recovery plans.

  For example, for Site Recovery Manager 8.2, see Site Recovery Manager Administration 8.2.

What to do next

After you run a recovery plan, either for a planned migration or a disaster recovery, perform a failback. See Perform a Failback After a Disaster Recovery or Planned Migration.

Perform a Failback After a Disaster Recovery or Planned Migration

After you run a recovery plan for a planned migration or disaster recovery of VMware Identity Manager, you can restore the pre-recovery site by performing a failback.

Performing a planned migration or a disaster recovery from site A to site B is a two-step process: recovery and reprotect. Recovery results in Recovery Time Objective (RTO) downtime. After the recovery from site A to site B, the recovered virtual machines run on site B without protection until you perform the reprotect operation.

Reprotect runs in parallel with VMware Identity Manager services. Therefore, end users do not experience further downtime during the reprotect operation.

Prerequisites

- You performed a recovery, either as part of a planned migration or as part of a disaster recovery.
- The original protected site, site A, is running.
- You did not run reprotect after the recovery.
- If you performed a disaster recovery, you must perform a planned migration when the hosts and datastores on the original protected site are running again.

Procedure

- Follow the instructions provided in *Site Recovery Manager Administration* about performing a failback.

  For example, for Site Recovery Manager 8.2, see Site Recovery Manager Administration 8.2

Installing Additional VMware Identity Manager Connector Appliances

5

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.

Read the following topics next:

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 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.

Install and Configure the Connector Virtual Appliance

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

Prerequisites

- Download the connector OVA file from the VMware Identity Manager product page on my.vmware.com.
- Ensure you have vSphere Client or vSphere Web Client.
- If using the vSphere Web Client, use either Firefox or Chrome browsers. Do not use Internet Explorer to deploy the OVA file.
- Identify the DNS records and host name to use for your appliance.

Procedure

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

2 Follow the wizard to deploy the template.

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

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

3 When the deployment is complete, select the 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.

4 To run the Setup wizard, point your browser to the connector URL displayed in the Console tab.

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

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

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

Option	Description
Appliance Administrator	Create the appliance administrator password. The user name is **admin** and cannot be changed. You use this account and password to log 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.

7 Click **Continue**.

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

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

The connector setup is complete.

What to do next

Click the link on the Setup is Complete page to go to the tenant administration console. Log in with the temporary administrator user name and password you received for your tenant. Then set up the directory connection.

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.
- 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.

Using the Built-in KDC

6

For Mobile SSO for iOS authentication on VMware Workspace ONE™ UEM managed iOS devices, you can use the built-in KDC. You manually initialize the Key Distribution Center (KDC) in the appliance before you enable the authentication method from the administration console.

Note When you integrate VMware Identity Manager with Workspace ONE UEM in a Windows environment, use the VMware Identity Manager KDC cloud hosted service, not the built-in KDC. Using KDC in the cloud requires selecting the appropriate realm name in the iOS authentication adapter page from the administration console. See the VMware Identity Manager Administration Guide.

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.

Download the KDC server root certificate from the VMware Identity Manager admin console to use in the Workspace ONE UEM configuration of the iOS device management profile.

Read the following topics next:

- Initialize the Key Distribution Center in the Appliance
- Creating Public DNS Entries for KDC with Built-in Kerberos
- Replace REALM

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 Chapter 6 Using the Built-in KDC.

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.

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. Two DNS records are required for each VMware Identity Manager site and two address entries.

Note An AAAA record is required for devices running on iOS 9 or are using T-Mobile as the carrier. 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 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`.

```
kdc.example.com.               1800 IN  A           1.2.3.4

kdc.example.com.               1800 IN  AAAA        ::ffff:1.2.3.4

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

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

Replace REALM

To change the realm after the initial configuration, you must add the new realm name and reinitialize the KDC service.

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.

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} --force`.

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

   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`.

Results

The realm name is updated in the iOS KdcKerberosAuthAdapter authentication method configuration page.

Monitoring VMware Identity Manager 7

Monitoring VMware Identity Manager is an important part of ensuring your Workspace ONE solution works correctly.

You can use third-party tools such as Nagios, Splunk, Symantec Altiris, Spotlight, Ignite, or Montastic. Consult your company's IT department for specific recommendations on monitoring tools if you do not already have a solution in place.

This document provides generic hardware load capacity recommendations and information about log files and URL endpoints. It does not explicitly cover how to configure a monitoring solution.

Read the following topics next:

- Hardware Load Capacity Monitoring Recommendations
- VMware Identity Manager URL Endpoints for Monitoring
- System Logging

Hardware Load Capacity Monitoring Recommendations

Use these monitoring standards to ensure server health.

Metrics to Capture

Hardware	Monitors
CPU	Usage
Memory	Usage
Hard Disk	Free space
Network	Usage

Alerts and Thresholds

VMware recommends analyzing each individual use case to determine the correct thresholds for individual environments.

Hardware	Alerts, Samples, Thresholds
CPU	Samples: 5 minute samples Threshold: 90% over 1 hour, 95 over 1 hour Alerts: 90% load is a warning, 95% is critical
Memory	Samples: 5 minute samples Threshold: 90% over 1 hour, 95 over 1 hour Alerts: 90% used is a warning, 95% used is critical
Hard Disk	Samples: 5 minute samples Threshold: 90% over 1 hour, 95 over 1 hour Alerts: 90% used is a warning, 95% used is critical
Network	Samples: 5 minute samples Threshold: 90% over 1 hour, 95 over 1 hour Alerts: 90% load is a warning, 95% is critical

Strategies for Capture

- VMware Identity Manager Linux Virtual Appliance: For a virtual appliance, the metrics are captured by the underlying virtual infrastructure utilizing tools such as vSphere or vRealize Operations.
- VMware Identity Manager on Windows: Install a monitoring agent that is supported for Windows servers and can capture these metrics. Additionally, for virtual servers, you can use tools native to vSphere to capture the relevant metrics.

VMware Identity Manager URL Endpoints for Monitoring

Monitor the listed URL endpoints for various VMware Identity Manager components to ensure a functional environment. Certain endpoints can also be used for load balancers to ensure the service is up for traffic.

Health Checks for Load Balancers

Component	Health Check	Expected Return	Notes
VMware Identity Manager Service	`/SAAS/API/1.0/REST/system/health/heartbeat`	String: ok Http: 200	Frequency every 30 seconds
	Android Mobile SSO - Certproxy: `:5262/system/health`	Http: 200	Frequency every 30 seconds
	iOS Mobile SSO - KDC: `TCP half-open to port 88`	Connection	Frequency every 30 seconds
	Certificate adapter: `:7443/SAAS/API/1.0/REST/system/health/heartbeat`	String: ok Http: 200	Frequency every 30 seconds

Component	Health Check	Expected Return	Notes
VMware Identity Manager Connector	`/hc/API/1.0/REST/system/health/allOk`	String: true Http: 200	Frequency every 30 seconds
Integration Broker	`/IB/API/RestServiceImpl.svc/ibhealthcheck`	String: All Ok Http: 200	Frequency every 30 seconds
	XenApp 7.x Integration: `/IB/API/RestServiceImpl.svc/hznxenapp/admin/xenfarminfo?computerName=&xenappversion=Version7x`	String: 'SiteName' Http: 200	Frequency every 5 minutes
	XenApp 6.x Integration: `/IB/API/RestServiceImpl.svc/hznxenapp/admin/xenfarminfo?computerName=&xenappversion=Version65orLater`	String: 'FarmName' Http: 200	Frequency every 5 minutes

The health checks for load balancers return simple values for easy parsing by network equipment.

Additional Health Checks for Monitoring

The health checks listed here can be consumed by monitoring solutions that have the ability to parse data and create dashboards. Set the frequency to every 5 minutes.

VMware Identity Manager Service Monitoring and Health

URL call: `/SAAS/jersey/manager/api/system/health`

or

`/SAAS/API/1.0/REST/system/health`

Raw output:


```
{
   "AnalyticsUrl":"unknown",
   "ElasticsearchServiceOk":"true",
   "EhCacheClusterPeers":"unknown",
   "ElasticsearchMasterNode":"unknown",
   "ElasticsearchIndicesCount":"unknown",
   "ElasticsearchDocsCount":"unknown",
   "AuditPollInterval":"0",
   "AnalyticsConnectionOk":"true",
   "EncryptionServiceVerified":"unknown",
   "FederationBrokerStatus":"unknown",
   "ServiceReadOnlyMode":"false",
```

```
    "ElasticsearchUnassignedShards":"unknown",
    "AuditWorkerThreadAlive":"true",
    "BuildVersion":"3.3.0.0 Build xxxxxxx",
    "AuditQueueSize":"0",
    "DatabaseStatus":"unknown",
    "HostName":"unknown",
    "ElasticsearchNodesCount":"unknown",
    "EncryptionStatus":"unknown",
    "FederationBrokerOk":"true",
    "EncryptionConnectionOk":"true",
    "EncryptionServiceImpl":"unknown",
    "ClusterId":"22f6e089-45df-41ab-9c8a-77f3e4589230",
    "EhCacheClusterDiagnostics":"unknown",
    "ElasticsearchNodesList":"unknown",
    "DatabaseConnectionOk":"true",
    "ElasticsearchHealth":"unknown",
    "StatusDate":"2018-08-06 19:14:40 UTC",
    "ClockSyncOk":"true",
    "MaintenanceMode":"false",
    "MessagingConnectionOk":"true",
    "fipsModeEnabled":"true",
    "ServiceVersion":"3.3.0",
    "AuditQueueSizeThreshold":"null",
    "IpAddress":"unknown",
    "AuditDisabled":"false",
    "AllOk":"true"
}
```


"AllOk"	"true", "false"	Roll-up health check to monitor overall health of VMware Identity Manager services
"MessagingConnectionOk"	"true", "false"	Verifies that all message producers and consumers are connected to RabbitMQ
"DatabaseConnectionOk"	"true", "false"	Verifies the connection to the database
"EncryptionConnectionOk"	"true", "false"	Verifies that the connection to the encryption service is okay and the master key store is okay
"AnalyticsConnectionOk"	"true", "false"	Verifies the connection to the analytics service
"FederationBrokerOk"	"true", "false"	Verifies the embedded auth adapters to ensure their subsystems are okay

Note The label "unknown" in the output indicates that the information is restricted. By default, sensitive information such as IP addresses and host names, is hidden. To display this information, see Displaying Additional Information in Health Check API.

URL call: `/catalog-portal/services/health`

This health check is specific for the user interface part of VMware Identity Manager.

Raw output:


```
{
    "status": "UP",
    "uiService": {
        "status": "UP"
    },
    "apiService": {
        "status": "UP"
    },
    "eucCacheEngine": {
        "status": "UP"
    },
    "cacheEngineClient": {
        "status": "UP"
    },
    "persistenceEngine": {
        "status": "UP",
        "database": "Microsoft SQL Server",
        "hello": 1
    },
    "tenantPersistenceEngine": {
        "status": "UP",
        "database": "Microsoft SQL Server",
        "hello": 1
    },
    "diskSpace": {
        "status": "UP",
        "total": 8460120064,
        "free": 4898279424,
        "threshold": 10485760
    }
}
```


"status"	"UP", "DOWN"	Roll-up health check to monitor overall health of the VMware Identity Manager user interface (UI)
"uiServer.status"	"UP", "DOWN"	UP if the main UI service is running
"apiService.status"	"UP", "DOWN"	UP if the main UI API service is running
"eucCacheEngine.status"	"UP", "DOWN"	UP if the Hazelcast cluster engine is running
"cacheEngineClient.status"	"UP", "DOWN"	UP if the Hazelcast client for the UI is running
"persistenceEngine.status"	"UP", "DOWN"	UP if the main database (SQL) is running
"tenantPersistenceEngine.status"	"UP", "DOWN"	UP if the main database (SQL) is running

"diskSpace.status"	"UP", "DOWN"	UP if the free disk space is greater than the threshold configured, 10 MB
"diskSpace.free"	Bytes	Space free in Bytes on the partition where the VMware Identity Manager UI is installed

VMware Identity Manager Connector Monitoring and Health

URL call: **`/hc/API/1.0/REST/system/health`**

Raw output:


```
{
       "HorizonDaaSSyncConfigurationStatus": "",
       "AppManagerServiceOk": "true",
       "DomainJoinEnabled": "false",
       "XenAppEnabled": "true",
       "ViewSyncConfigurationStatus": "",
       "ThinAppServiceOk": "true",
       "ThinAppSyncConfigurationStatus": "unknown",
       "Activated": "true",
       "XenAppServiceOk": "false",
       "DirectoryServiceStatus": "Connection test successful",
        "BuildVersion": "2017.1.1.0 Build 5077496",
       "ThinAppServiceStatus": "unknown",
       "XenAppServiceStatus": "A problem was encountered Sync Integration Broker",
       "HostName": "hostname.company.local",
       "NumberOfWarnAlerts": "0",
       "JoinedDomain": "true",
       "XenAppSyncConfigurationStatus": "Sync configured (manually)",
       "DirectorySyncConfigurationStatus": "Sync configured (manually)",
       "NumberOfErrorAlerts": "0",
       "DirectoryServiceOk": "true",
       "HorizonDaaSTenantOk": "true",
       "ThinAppDirectoryPath": "",
       "StatusDate": "2017-06-27 10:52:59 EDT",
       "ViewSyncEnabled": "false",
       "ViewServiceOk": "true",
       "HorizonDaaSEnabled": "false",
       "AppManagerUrl": "https://workspaceurl.com/SAAS/t/qwe12312qw/",
       "HorizonDaaSServiceStatus": "unknown",
       "DirectoryConnection": "ldap:///ldapcall",
       "ServiceVersion": "VMware-C2-2017.1.1.0 Build 5077496",
       "IpAddress": "169.118.86.105",
       "DomainJoinStatus": "Domain: customerdomainname",
       "AllOk": "false",
       "ViewServiceStatus": "unknown",
       "ThinAppEnabled": "false",
       "XenAppSyncSsoBroker": "integrationbrokersso:443 / integrationbrokersync:443"
}
```

"AllOk"	"true", "false"	Roll-up health check to monitor overall health of VMware Identity Manager Connector Services.
"ViewServiceOk"	"true", "false"	True, if connection to the View Broker is successful. This attribute will be true if View sync is disabled.
"HorizonDaaSTenantOk"	"true", "false"	True, if connection to Horizon Cloud is successful. This attribute will be true if Horizon Cloud sync is disabled.
"DirectoryServiceOk"	"true", "false"	True, if connection to the directory is successful. This attribute will be true if directory sync is disabled.
"XenAppServiceOk"	"true", "false"	True, if connection to the Citrix server is successful. This attribute will be true if Citrix server is disabled.
"ThinAppServiceOk"	"true", "false"	True, if connection to the ThinApp packaged applications service is successful. This attribute will be true if packaged applications are disabled.
"AppManagerServiceOk"	"true", "false"	True, if able to authenticate correctly to the AppManager.
"NumberOfWarnAlerts"	0 - 1000	Number of warning alerts that triggered on this Connector. These are available on the Connector Sync Log as “Notes.” They can indicate that a resource was synced in that included a user or group that is not in VMware Identity Manager. Depending on the configuration, this may be by design. The counter continues to increment on each sync until Warn and Error alerts equal 1000 and an administrator clears the alerts.
"NumberOfErrorAlerts"	0 - 1000	Number of error alerts that triggered on this Connector. These are available on the Connector Sync Log as “Error.” They can indicate that a sync failed. The counter continues to increment on each sync until Warn and Error alerts equal 1000 and an administrator clears the alerts.

VMware Identity Manager Integration Broker Monitoring and Health

URL call: `/IB/API/RestServiceImpl.svc/ibhealthcheck`

Raw output:

```
“All Ok”
```

This health check verifies that all the software on the Integration Broker is responding properly. It returns a 200 response with the string "All Ok".

VMware Identity Manager Integration Broker Monitoring and Health with Citrix XenApp 7.x

URL call: `/IB/API/RestServiceImpl.svc/hznxenapp/admin/xenfarminfo?computerName=&xenappversion=Version7x`

This pulls back information from an API call to Citrix. Monitoring can ensure that the values are consistent.

Raw output:

```
[{
     \ “ConfigurationLoggingServiceGroupUid \ “:  \ “5e2a5602 - 45a8 - 4b56 - 92e6 -
9fae5a3ff459 \ “,
     \ “ConfigurationServiceGroupUid \ “:  \ “620d7c6e - b7c1 - 4ee7 - b192 - d00764f477e7 \
“,         \ “DelegatedAdministrationServiceGroupUid \ “:  \ “0a59914d - 4b6e - 4cca - bbaa -
a095067092e3 \ “,
     \ “LicenseServerName \ “:  \ “xd.hs.trcint.com \ “,
     \ “LicenseServerPort \ “:  \ “27000 \ “,
     \ “LicenseServerUri \ “:  \ “https:  \  /  \  / xd.hs.domain.com: 8083 \  /  \ “,
     \ “LicensingBurnIn \ “:  \ “2014.0815 \ “,
     \ “LicensingBurnInDate \ “:  \ “8 \  / 14 \  / 2014 5: 00: 00 PM \ “,
     \ “LicensingModel \ “:  \ “UserDevice \ “,
    \ “MetadataMap \ “:  \ “System.Collections.Generic.Dictionary
`2[System.String,System.String]\“,
    \“PrimaryZoneName\“:\“\”,
    \“PrimaryZoneUid\“:\“00000000-0000-0000-0000-000000000000\“,
    \“ProductCode\“:\“XDT\“,
    \“ProductEdition\“:\“PLT\“,
    \“ProductVersion\“:\“7.6\“,
    \“SiteGuid\“:\“0c074098-02d2-47cf-aa87-7e3asdsad7c\“,
    \“SiteName\“:\“customer\“
}]
```

Raw output exception:

```
{“ExceptionType”:“System.Management.Automation.CmdletInvocationException”,“Message”:“An
invalid URL was given for the service.  The value given was ‘mit-
xen751.hs.trcint.com’.\u000d\u000a    The reason given was: Failed to connect to back-
end server ‘mit-xen751.hs.trcint.com’ on port 80 using binding WSHttp. The server may
be off-line or may not be running the appropriate service\u000d\u000a\u0009There was
no endpoint listening at http:\/\/mit-xen751.hs.trcint.com\/Citrix\/ConfigurationContract\/v2
that could accept the message. This is often caused by an incorrect address or
SOAP action. See InnerException, if present, for more details.\u000d\u000a\u0009The
remote name could not be resolved: ‘mit-xen751.hs.trcint.com’.“,”StackTrace”:”
at System.Management.Automation.Internal.PipelineProcessor.SynchronousExecuteEnumerate(Object
input, Hashtable errorResults, Boolean enumerate)\u000d\u000a
at System.Management.Automation.Internal.PipelineProcessor.SynchronousExecute(Array
input, Hashtable errorResults)\u000d\u000a   at
System.Management.Automation.Runspaces.LocalPipeline.InvokeHelper()\u000d\u000a   at
System.Management.Automation.Runspaces.LocalPipeline.InvokeThreadProc()“}
```

VMware Identity Manager Integration Broker Monitoring and Health with Citrix XenApp 6.x

URL call: `/IB/API/RestServiceImpl.svc/hznxenapp/admin/xenfarminfo?computerName=&xenappversion=Version65orLater`

This pulls back information from an API call to Citrix. Monitoring can ensure that the values are consistent.

Raw output:

```
"[{
       \ "FarmName \ ":  \ "NewFarm \ ",
     \ "ServerVersion \ ":  \ "6.5.0 \ ",
     \ "AdministratorType \ ":  \ "Full \ ",
     \ "SessionCount \ ":  \ "0 \ ",
     \ "MachineName \ ":  \ "XENAPPTEST \ "
    }]"
```

Displaying Additional Information in Health Check API

You can control whether sensitive information, such as IP addresses and host names, is displayed in the output of the health check APIs `https://<VIDM_FQDN>/SAAS/jersey/manager/api/system/health` and `https://<VIDM_FQDN>/SAAS/API/1.0/REST/system/health`. By default, the API output does not include this information.

The `service.health.check.basic` property in the `runtime-config.properties` file controls this setting. When the property is set to **`true`**, only basic information is displayed and sensitive information is hidden. The label `"unknown"` in the output indicates that the information is restricted. For example:

```
AnalyticsUrl:    "unknown"
ElasticsearchServiceOk:    "true"
EhCacheClusterPeers:    "unknown"
ElasticsearchMasterNode:    "unknown"
ElasticsearchIndicesCount    "unknown"
ElasticsearchDocsCount:    "unknown"
AuditPollInterval:    "1000"
AnalyticsConnectionOk:    "true"
...
IpAddress:    "unknown"
AuditDisabled:    "false"
AllOk:    "true"
```

When the property is set to **`false`**, all available information is displayed. For example:

```
AnalyticsUrl: "http://198.51.100.0"
ElasticsearchServiceOk: "true"
EhCacheClusterPeers: ""
ElasticsearchMasterNode: "198.51.100.1"
ElasticsearchIndicesCount: "13"
ElasticsearchDocsCount: "11173"
```

```
AuditPollInterval: "1000"
AnalyticsConnectionOk: "true"
...
IpAddress: "198.51.100.2"
AuditDisabled: "false"
AllOk: "true"
```

By default, the property is set to **`true`**.

Note If you have set up a VMware Identity Manager cluster, if you change the property ensure that you make the change in all nodes in the cluster.

Procedure

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

2 Edit the `/usr/local/horizon/conf/runtime-config.properties` file and set the value of the `service.health.check.basic` property to **`true`** or **`false`**.

Option	Description
true	Displays only basic information. Sensitive information is hidden and the label `Unknown` appears in its place.
false	Displays all available information

3 Save the file.

4 Restart the service.

```
service horizon-workspace restart
```

5 If you have set up a VMware Identity Manager cluster, make these changes in each node of the cluster.

System Logging

Logging from the VMware Identity Manager service and the VMware Identity Manager connector components is available using syslog. The Integration Broker component logs locally. The logs can be collected and reviewed on the server or through a central logging service such as vRealize Log Insight or Splunk.

VMware Identity Manager Service and Connector Logging

Log Locations

Most service and connector logs are located in the following location:

- VMware Identity Manager Linux virtual appliance: `/opt/vmware/horizon/workspace/logs/`
- VMware Identity Manager on Windows: `\<Install_Dir>\VMware Identity Manager\opt\vmware\horizon\workspace\logs`

Log	Purpose
greenbox_web.log	Log which contains all user interface interactions for web and mobile
horizon.log	VMware Identity Manager service log which includes Identity Adapters, RabbitMQ, Elasticsearch, Ehcache, and other subsystems
connector.log	VMware Identity Manager connector log for all authentication methods and integrations with Horizon and Citrix
cert-proxy.log	VMware Identity Manager service CertProxy component for Android Mobile SSO
configurator.log	Requests that the Configurator receives from the REST client and the Web interface
/opt/vmware/var/log/update.log	A record of output messages related to update requests during an upgrade of VMware Identity Manager
/opt/vmware/var/log/vami/	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.
catalina.log	Apache Tomcat records of messages that are not recorded in other log files
/var/log/messages	iOS KDC logs for Mobile SSO

Syslog Server Setup

To set up a syslog server, see Configure a Syslog Server.

Integration Broker Logging

Integration Broker logs are located in the following location:

C:\ProgramData\VMware\HorizonIntegrationBroker

The logs are captured by day and contain all REST API calls made to and by Integration Broker.

Setting Rate Limits

8

You can set rate limits on the VMware Identity Manager service and the VMware Identity Manager connector.

Read the following topics next:

- Setting Rate Limits on the VMware Identity Manager Service
- Setting Rate Limits on the VMware Identity Manager Connector

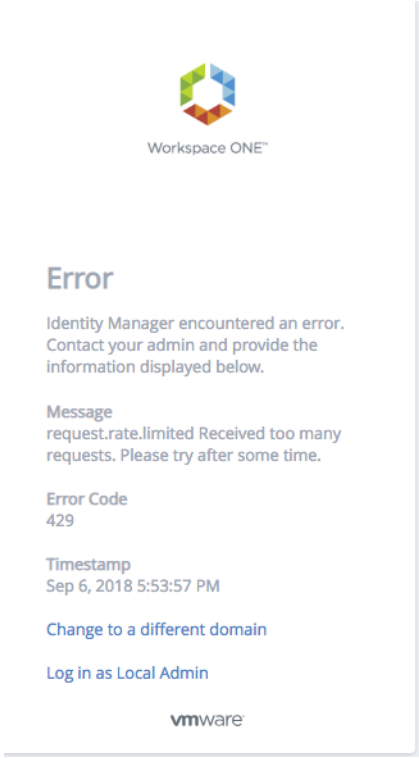
Setting Rate Limits on the VMware Identity Manager Service

You can set limits on the number of login, launch, and WS-Fed requests that can be made per minute to the VMware Identity Manager service. When the limit is reached, subsequent requests are denied. Setting rate limits helps prevent overload of the system.

For example, if you set the rate limit for login requests to 100, the first 100 login requests per minute are accepted but requests 101-n are denied.

For a VMware Identity Manager cluster, the rate limit applies to each node in the cluster. For example, if you set the login request rate limit to 100 for a cluster that has NodeA, NodeB, and NodeC, NodeA can process 100 login requests per minute, NodeB can process 100 login requests per minute, and NodeC can process 100 login requests per minute. You cannot set separate login limits per node.

When the limit is reached and requests are denied, end users see the following error message:



No rate limits are set by default.

You set rate limits using a REST API. Use a REST client such as Postman to make the calls to the VMware Identity Manager service. The changes take effect in a few minutes.

Setting Rate Limits

Use this API to set rate limits for the VMware Identity Manager service.

Endpoint: `https://hostname/SAAS/jersey/manager/api/system/tuning/resiliency/tenant/orgResiliencyConfiguration?tenantId=tenantId`

Method: PUT

Description: Sets the maximum number of login, launch, and WS-Fed requests allowed per minute by the VMware Identity Manager service.

Headers:

Content-Type	`application/vnd.vmware.horizon.manager.system.tuning.resiliency.config+json;charset=UTF-8`
Accept	`application/vnd.vmware.horizon.manager.system.tuning.resiliency.config+json`
Authorization	`HZN cookie_value` To get the *cookie_value*, log into the VMware Identity Manager service as the tenant administrator, that is, the admin user that is created when you first install VMware Identity Manager, and obtain the value of the HZN cookie from your browser's cookie cache.

Path Parameters:

`hostname`	The fully-qualified domain name of the VMware Identity Manager service or load balancer.
`tenantId`	The tenantId of the VMware Identity Manager service. The tenant ID is the tenant name that appears in the top-right corner of the VMware Identity Manager console.

Request Body:

```
{
"config": {
          "rateLimitingDisabled": false,
          "rateLimits": {
              "login": {
                  "requestsPerMinute": n
              },
              "launch": {
                  "requestsPerMinute": n
              },
              "ws-fed": {
          "requestsPerMinute": n
          }
      }
  }
  }
```

Request Body Parameters

login requestsPerMinute	Specify the maximum number of login requests allowed per minute. **Note** Take into account that multiple API requests might be needed for a login request to complete and each API call counts towards the rate limits. For example, password authentication involves two API calls, one to render the login page and the second to submit credentials.
launch requestsPerMinute	Specify the maximum number of launch requests allowed per minute.
ws-fed requestsPerMinute	Specify the maximum number of WS-Fed requests allowed per minute. WS-Fed rate limits are for Active Logon configurations only.

Viewing Rate Limits

Use this API to view rate limits that are set for the VMware Identity Manager service.

Endpoint: `https://hostname/SAAS/jersey/manager/api/system/tuning/resiliency/tenant/orgResiliencyConfiguration?tenantId=tenantId`

Method: GET

Description: Retrieves the rate limits that are currently set for login, launch, and WS-Fed requests for the VMware Identity Manager service.

Headers:

Authorization	`HZN cookie_value` To get the *cookie_value*, log into the VMware Identity Manager service as the tenant administrator, that is, the admin user that is created when you first install VMware Identity Manager, and obtain the value of the HZN cookie from your browser's cookie cache.

Path Parameters:

`hostname`	The fully-qualified domain name of the VMware Identity Manager service or load balancer.
`tenantId`	The tenant Id of the VMware Identity Manager service. The tenant ID is the tenant name that appears in the top-right corner of the VMware Identity Manager console.

Sample Output:

```
{
"config": {
          "rateLimitingDisabled": false,
          "rateLimits": {
              "login": {
                  "requestsPerMinute": 100
              },
              "launch": {
                  "requestsPerMinute": 100
              },
              "ws-fed": {
          "requestsPerMinute": 100
          }
      }
  }
  }
```

login requestsPerMinute	The maximum number of login requests allowed per minute.
launch requestsPerMinute	The maximum number of launch requests allowed per minute.
ws-fed requestsPerMinute	The maximum number of WS-Fed requests allowed per minute. WS-Fed rate limits are for Active Logon configurations only.

Setting Rate Limits on the VMware Identity Manager Connector

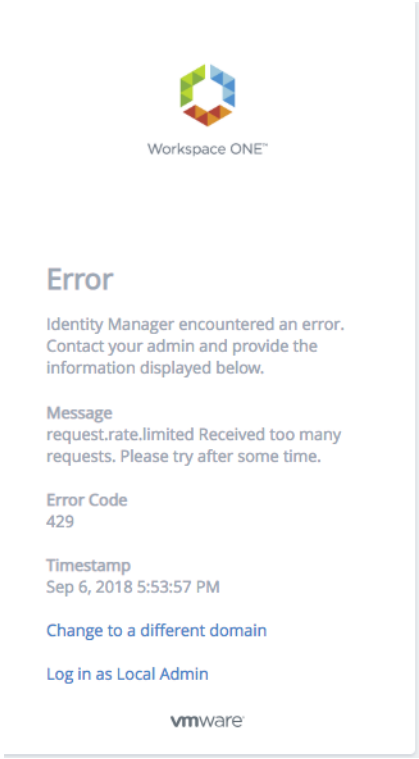
Just as you can set rate limits on the VMware Identity Manager service, you can set rate limits on the VMware Identity Manager connector.

For the connector, you can set a limit on the number of login requests that are allowed per minute. When the limit is reached, subsequent requests are denied. Setting rate limits helps prevent overload of the system.

For example, if you set the rate limit for login requests to 100, the first 100 login requests per minute are accepted but requests 101-n are denied.

For a VMware Identity Manager connector cluster, the limit applies to each node in the cluster. For example, if you set the login request rate limit to 100 for a cluster that has NodeA, NodeB, and NodeC, NodeA can process 100 login requests per minute, NodeB can process 100 login requests per minute, and NodeC can process 100 login requests per minute. You cannot set separate login limits per node.

When the limit is reached and requests are denied, end users see the following error message:



No rate limits are set by default.

You set rate limits using a REST API. Use a REST client such as Postman to make the calls to the VMware Identity Manager service.

Changes take effect after about an hour. Restart the connector if you want the changes to take effect immediately.

To restart the Linux-based connector virtual appliance, log in to the virtual appliance and run the following command:

```
service horizon-workspace restart
```

To restart the Windows connector, run the following script:

```
install_dir\usr\local\horizon\scripts\horizonService.bat restart
```

Setting Rate Limits

Use this API to set rate limits for the VMware Identity Manager connector.

Endpoint: `https://hostname/SAAS/jersey/manager/api/system/tuning/resiliency/tenant/orgResiliencyConnectorConfiguration?tenantId=tenantId`

Method: PUT

Description: Sets the maximum number of login requests allowed per minute by the VMware Identity Manager connector.

Headers:

Content-Type	`application/vnd.vmware.horizon.manager.system.tuning.resiliency.config+json;charset=UTF-8`
Accept	`application/vnd.vmware.horizon.manager.system.tuning.resiliency.config+json`
Authorization	`HZN cookie_value` To get the *cookie_value*, log into the VMware Identity Manager service as the tenant administrator, that is, the admin user that is created when you first install VMware Identity Manager, and obtain the value of the HZN cookie from your browser's cookie cache.

Path Parameters:

`hostname`	The fully-qualified domain name of the VMware Identity Manager service or load balancer.
`tenantId`	The tenant ID of the VMware Identity Manager service. The tenant ID is the tenant name that appears in the top-right corner of the VMware Identity Manager console.

Request Body:

```
{
"config": {
          "rateLimitingDisabled": false,
          "rateLimits": {
              "login": {
                  "requestsPerMinute": n
              }
     }
  }
  }
```

Request Body Parameters

login requestsPerMinute	Specifiy the maximum number of login requests allowed per minute. **Note** Take into account that multiple API requests might be needed for a login request to complete and each API call counts towards the rate limits. For example, password authentication involves two API calls, one to render the login page and the second to submit credentials.

Viewing Rate Limits

Use this API to view the rate limits that are set currently on the VMware Identity Manager connector.

Endpoint: `https://hostname/SAAS/jersey/manager/api/system/tuning/resiliency/tenant/orgResiliencyConnectorConfiguration?tenantId=tenantId`

Method: GET

Description: Retrieves the rate limits that are currently set for login requests for the VMware Identity Manager connector.

Headers:

Authorization	`HZN cookie_value` To get the *`cookie_value`*, log into the VMware Identity Manager service as the tenant administrator, that is, the admin user that is created when you first install VMware Identity Manager, and obtain the value of the HZN cookie from your browser's cookie cache.

Path Parameters:

`hostname`	The fully-qualified domain name of the VMware Identity Manager service or load balancer.
`tenantId`	The tenant Id of the VMware Identity Manager service. The tenant ID is the tenant name that appears in the top-right corner of the VMware Identity Manager console.

Sample Output:

```
{
"config": {
          "rateLimitingDisabled": false,
          "rateLimits": {
              "login": {
                  "requestsPerMinute": 100
              }
      }
  }
  }
```

login requestsPerMinute	The maximum number of login requests allowed per minute.

Troubleshooting Installation and Configuration

9

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

Read the following topics next:

- Users Unable to Launch Applications or Incorrect Authentication Method Applied in Load-Balanced Environments
- Users Unable to Launch Applications in Load-balanced Environment
- Group Does Not Display Any Members after Directory Sync

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
```

Users Unable to Launch Applications in Load-balanced Environment

Users are unable to launch applications from the Workspace ONE app or portal in a load-balanced VMware Identity Manager deployment.

Problem

Users are unable to launch applications from the Workspace ONE portal or app if their client IP address is determined incorrectly. This problem can occur in load-balanced VMware Identity Manager deployments if the X-Forwarded-For (XFF) header contains incorrect IP addresses.

Check the Audit Events launch report in the Dashboard to verify that the client IP address is being resolved correctly. If it is not being resolved correctly, follow this procedure to fix the problem.

Solution

To resolve the issue, first get the list of IP addresses listed in the XFF header by using the `clientipresolutioninfo` REST API and check the response. If it returns the IP address of the load balancer or VMware Identity Manager service node, then set the `service.ipsToIgnoreInXffHeader` property in the `runtime-config.properties` file to filter out the unwanted IP addresses.

To get the list of IP addresses in the XFF header, use a REST client such as Postman to run the following REST API while logged in to the VMware Identity Manager service as the tenant administrator:

Method: `GET`

Path: `/clientipresolutioninfo`

Authorization: `HZN` *`cookie_value`*

Note you can get the `HZN` cookie value by logging into the VMware Identity Manager service as the tenant administrator, then accessing your browser's cookie cache.

Response Media Type: `application/vnd.vmware.horizon.manager.clientipresolutionconfig+json`

Sample JSON response:

```
{
"xffHeaderIpList":["10.112.68.252"], // the IPs part of XFF header
"numberOfLoadBalancers":0, // number of load balancers configured in runtime-config.properties
"configuredIpToIgnoreList":"10.112.68.255", // the list of ips or subnets to ignore as
configured in runtime-config.properties
"clientIpDetermined":"10.112.68.252", // the client IP determined to be used finally for
login/access policy
"_links":{}
}
```

From the output, determine which IP addresses are not needed, then edit the `runtime-config.properties` file to filter them out.

1 Log in to the VMware Identity Manager virtual appliance.

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

```
service.ipsToIgnoreInXffHeader IPsToIgnore
```

where *`IPsToIgnore`* is a comma-separated list of IP addresses to ignore in the XFF header.

3 Restart the service.

```
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 VMware Identity Manager console, delete the group, add it again in the sync settings, and sync the directory again.