

# Installing and Configuring VMware Identity Manager

VMware Identity Manager 2.6

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

EN-002015-01

**vmware**<sup>®</sup>

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

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

The VMware Web site also provides the latest product updates.

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

[docfeedback@vmware.com](mailto:docfeedback@vmware.com)

Copyright © 2013 – 2016 VMware, Inc. All rights reserved. [Copyright and trademark information.](#)

**VMware, Inc.**  
3401 Hillview Ave.  
Palo Alto, CA 94304  
[www.vmware.com](http://www.vmware.com)

# Contents

About Installing and Configuring VMware Identity Manager	5
<b>1</b> Preparing to Install VMware Identity Manager	7
System and Network Configuration Requirements	9
Preparing to Deploy VMware Identity Manager	12
Create DNS Records and IP Addresses	12
Database Options with VMware Identity Manager	13
Connecting to Active Directory	13
Deployment Checklists	13
Customer Experience Improvement Program	15
<b>2</b> Deploying VMware Identity Manager	17
Install the VMware Identity Manager OVA File	17
(Optional) Add IP Pools	19
Configure VMware Identity Manager Settings	19
Setting Proxy Server Settings for VMware Identity Manager	25
Enter the License Key	25
<b>3</b> Managing Appliance System Configuration	
Settings	27
Change Appliance Configuration Settings	28
Connecting to the Database	28
Configure a Microsoft SQL Database	28
Configure an Oracle Database	29
Configure a PostgreSQL Database	31
Add an External Database to the VMware Identity Manager Appliance	32
Using SSL Certificates	33
Apply Public Certificate Authority	34
Adding SSL Certificates	35
Modifying the VMware Identity Manager Service URL	35
Modifying the Connector URL	36
Enable the Syslog Server	36
Log File Information	37
Collect Log Information	37
Manage Your Appliance Passwords	38
Configure SMTP Settings	38
<b>4</b> Integrating with Active Directory	39
Important Concepts Related to Active Directory	39
Active Directory Environments	40

About Domain Controller Selection (domain_krb.properties file)	42
Overriding the Default Subnet Selection	44
Editing the domain_krb.properties file	44
Troubleshooting domain_krb.properties	45
Managing User Attributes that Sync from Active Directory	45
Select Attributes to Sync with Directory	46
Joining a Domain	47
Configure Active Directory Connection to the Service	47
<b>5 Advanced Configuration for the VMware Identity Manager Appliance</b>	<b>53</b>
Using a Load Balancer to Enable External Access to the VMware Identity Manager	53
Apply VMware Identity Manager Root Certificate to the Load Balancer	55
Apply Load Balancer Root Certificate to VMware Identity Manager	56
Deploying Access Point for Reverse Proxy	56
Setting Proxy Server Settings for VMware Identity Manager	57
Configuring Redundancy	57
Configuring Failover and Redundancy	57
Enabling Directory Sync on Another Instance in the Event of a Failure	61
Adding a Directory After Configuring Failover and Redundancy	62
Deploying VMware Identity Manager in Secondary Data Center with Active-Active Read-Only Capability	63
Setting Up a Secondary Data Center	64
<b>6 Installing Additional Connector Appliances</b>	<b>69</b>
Generate Activation Code for Connector	70
Deploy the Connector OVA File	70
Configure Connector Settings	71
<b>7 Preparing to Use Kerberos Authentication on iOS Devices</b>	<b>73</b>
Pre- KDC Configuration Decisions	73
Initialize the Key Distribution Center in the Appliance	74
Creating Public DNS Entries for KDC with Built-in Kerberos	75
<b>Index</b>	<b>77</b>

# About Installing and Configuring VMware Identity Manager

---

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

## Intended Audience

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



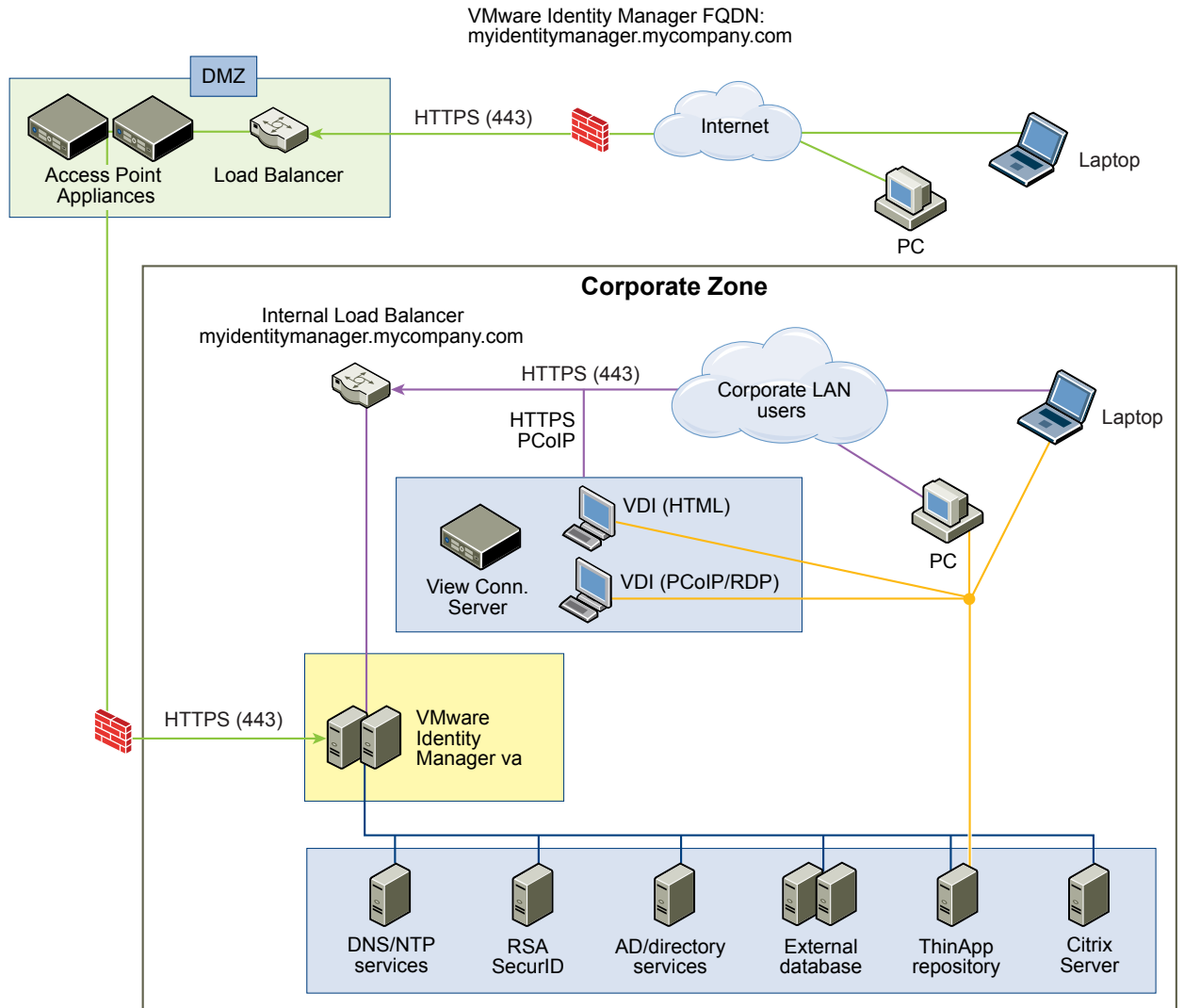
# Preparing to Install VMware Identity Manager

---

# 1

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

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



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

This chapter includes the following topics:

- [“System and Network Configuration Requirements,”](#) on page 9
- [“Preparing to Deploy VMware Identity Manager,”](#) on page 12
- [“Customer Experience Improvement Program,”](#) on page 15



## System and Network Configuration Requirements

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

### Supported vSphere and ESX Versions

The following versions of vSphere and ESX server are supported:

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

### VMware Identity Manager Virtual Appliance Requirements

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

Component	Minimum Requirement
CPU	2
Random-access memory	6GB
Disk space	36GB
Database	<ul style="list-style-type: none"> <li>■ A PostgreSQL database is included in the VMware Identity Manager virtual appliance, and you can use an external database server. For information about specific database versions and service pack configurations supported with VMware Identity Manager, see the VMware Product Interoperability Matrix at <a href="http://www.vmware.com/resources/compatibility/sim/interop_matrix.php">http://www.vmware.com/resources/compatibility/sim/interop_matrix.php</a>.</li> <li>■ External database sizing information: 64GB for first 100,000 users. Add 20GB for each additional 10,000 users.</li> <li>■ Storage: 32GB</li> </ul>

### 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	Access Point 2.6 supports reverse proxy functionality to allow users to securely access VMware Identity Manager unified catalog remotely. Access Point 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 below. Your deployment might include only a subset of these. Here are two potential scenarios:

- To sync users and groups, 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	Source	Target	Description
443	Load Balancer	VMware Identity Manager virtual appliance	HTTPS
88	Load Balancer	VMware Identity Manager virtual appliance	TCP Port used for Kerberos traffic from iOS devices to the Built-in KDC.
443	VMware Identity Manager virtual appliance	VMware Identity Manager virtual appliance	HTTPS
443	Browsers	VMware Identity Manager virtual appliance	HTTPS
443	VMware Identity Manager virtual appliance	vapp-updates.vmware.com	Access to the upgrade server.
8443	Browsers	VMware Identity Manager virtual appliance	Administrator Port HTTPS
25	VMware Identity Manager virtual appliance	SMTP	TCP port to relay outbound mail
389, 636, 3268, 3269	VMware Identity Manager virtual appliance	Active Directory	Default values are shown. These ports are configurable.
445	VMware Identity Manager virtual appliance	VMware ThinApp repository	Access to ThinApp repository
5500	VMware Identity Manager virtual appliance	RSA SecurID system	Default value is shown. This port is configurable
53	VMware Identity Manager virtual appliance	DNS server	TCP/UDP Every virtual appliance must have access to the DNS server on port 53 and allow incoming SSH traffic on port 22
88, 464, 135	VMware Identity Manager virtual appliance	Domain controller	TCP/UDP
TCP: 9300-9400 UDP: 54328	VMware Identity Manager virtual appliance	VMware Identity Manager virtual appliance	Audit needs
5432	VMware Identity Manager virtual appliance	Database	The PostgreSQL default port is 5432. The Oracle default port is 1521
389, 443	VMware Identity Manager virtual appliance	View server	Access to View server

## Hardware Requirements for ESX Server

Ensure that the environment for the host and the vSphere instance that runs the VMware Identity Manager virtual appliance meets the minimum hardware requirements. Storage requirements vary per deployment based on the number of users.

**NOTE** You must turn on time sync at the ESX host level using an NTP server. Otherwise, a time drift will occur 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.

Component	Minimum Requirement
Processor	2 Intel Quad Cores, 3.0GHz, 4MB Cache
RAM	16GB DDR2 1066 MHz, ECC and registered
On-board LAN	One 10/100/1000Base-TX port
Storage	500GB

## Active Directory

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

## Supported Web Browsers to Access the Administration Console

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

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

---

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

---

## Supported Browsers to Access the User's My Apps Portal

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

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

---

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

---

## 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 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](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 appliance. Because each company administers their IP addresses and DNS records differently, before you begin your installation, request the DNS record and IP addresses to use.

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

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

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

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

This example shows reverse DNS records and IP addresses.

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

IP Address	Resource Type	Domain Name
128.28.10.in-addr.arpa.	IN	PTR myidentitymanager.company.com

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

## Using a Unix/Linux-based DNS Server

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

## Database Options with VMware Identity Manager

Set up VMware Identity Manager with an external database to store and organize server data. If you cannot use an external database, you can use the internal vPostgres database that is embedded in the appliance.

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 an external Microsoft SQL database server, Oracle database server, or an external vPostgres database server to set up a high availability external database environment. See [“Connecting to the Database,”](#) on page 28.

The embedded vPostgres database configuration can be used for small deployments. The internal database does not require any additional configuration outside VMware Identity Manager, but it is recommended that you configure your internal database for high availability. See KB 2094258.

## Connecting to Active Directory

VMware Identity Manager uses your Active 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. To sync users and groups, the VMware Identity Manager virtual appliance must connect to Active Directory.

Your Active Directory must be accessible in the same LAN network as the VMware Identity Manager virtual appliance. See [Chapter 4, “Integrating with Active Directory,”](#) on page 39.

## Deployment Checklists

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

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

### Information for Fully Qualified Domain Name

See [“Using a Load Balancer to Enable External Access to the VMware Identity Manager,”](#) on page 53 for information.

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

Information to Gather	List the Information
VMware Identity Manager FQDN	

### Network Information for VMware Identity Manager Virtual Appliance

**Table 1-4.** Network Information Checklist

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

## Active Directory Domain Controller

**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.	

## SSL Certificates

**Table 1-6.** SSL Certificate Information Checklist

Information to Gather	List the Information
SSL certificate	
Private key	
<b>NOTE</b> You can add an SSL certificate after you deploy the VMware Identity Manager virtual appliance.	

## License Key

**Table 1-7.** VMware Identity Manager License Key Information Checklist

Information to Gather	List the Information
License key	
<b>NOTE</b> The License key information is entered in the administration console in the <b>Appliance Settings &gt; License</b> page after the installation is complete.	

## External Database

**Table 1-8.** External Database Information Checklist

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

## Appliance Administrator Passwords

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

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

**Table 1-9.** Administrator Passwords

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

## Customer Experience Improvement Program

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

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

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

---

**NOTE** If your network is configured to access the Internet through HTTP proxy, to send this information, you must adjust the proxy settings in the VMware Identity Manager virtual appliance. See [“Setting Proxy Server Settings for VMware Identity Manager,”](#) on page 25.

---





# Deploying VMware Identity Manager

---

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

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

Use the information in the deployment checklist to complete the installation. See [“Deployment Checklists,”](#) on page 13.

This chapter includes the following topics:

- [“Install the VMware Identity Manager OVA File,”](#) on page 17
- [“\(Optional\) Add IP Pools,”](#) on page 19
- [“Configure VMware Identity Manager Settings,”](#) on page 19
- [“Setting Proxy Server Settings for VMware Identity Manager,”](#) on page 25
- [“Enter the License Key,”](#) on page 25

## Install the VMware Identity Manager OVA File

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

---

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

---

### Prerequisites

Review and [Chapter 1, “Preparing to Install VMware Identity Manager,”](#) on page 7.

### Procedure

- 1 Download the VMware Identity Manager OVA file from My VMware.
- 2 Log in to the vSphere Client or the vSphere Web Client.
- 3 Select **File > Deploy OVF Template**.

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

Page	Description
<b>Source</b>	Browse to the OVA package location, or enter a specific URL.
<b>OVF Template Details</b>	Review the product details, including version and size requirements.
<b>End User License Agreement</b>	Read the End User License Agreement and click <b>Accept</b> .
<b>Name and Location</b>	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.
<b>Host / Cluster</b>	Select the host or cluster in which to run the virtual appliance.
<b>Resource Pool</b>	Select the resource pool.
<b>Storage</b>	Select the storage for the virtual appliance files. You can also select a VM Storage Profile.
<b>Disk Format</b>	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.
<b>Network Mapping</b>	Map the networks used in VMware Identity Manager to networks in your inventory.
<b>Properties</b>	<p>a In the <b>Timezone setting</b> field, select the correct time zone.</p> <p>b The <b>Customer Experience Improvement Program</b> 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.</p> <p>c In the <b>Host Name (FQDN)</b> text box, enter the host name to use. If this is blank, reverse DNS is used to look up the host name.</p> <p>d Configure the networking properties.</p> <ul style="list-style-type: none"> <li>■ To configure a static IP address for VMware Identity Manager, enter the address for the <b>Default Gateway</b>, <b>DNS</b>, <b>IP Address</b>, and <b>Netmask</b> fields. <b>IMPORTANT</b> If any of the four address fields, including <b>Host Name</b>, are left blank, DHCP is used.</li> <li>■ To configure DHCP, leave the address fields blank.</li> </ul> <p><b>NOTE</b> The <b>Domain Name</b> and <b>Domain Search Path</b> fields are not used. You can leave these blank.</p> <p>(Optional) After VMware Identity Manager is installed, you can configure IP Pools. See <a href="#">“(Optional) Add IP Pools,”</a> on page 19.</p>
<b>Ready to Complete</b>	Review your selections and click <b>Finish</b> .

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

- 5 When the deployment is complete, click **Close** in the progress dialog box.
- 6 Select the VMware Identity Manager virtual appliance you deployed, right-click, and select **Power > Power on**.

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

#### What to do next

- (Optional) Add IP Pools.

- Configure VMware Identity Manager settings, including connecting to Active Directory and selecting users and groups to sync to VMware Identity Manager.

## (Optional) Add IP Pools

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

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

### Prerequisites

The virtual appliance must be powered off.

### Procedure

- 1 In the vSphere Client or the vSphere Web Client, right-click the VMware Identity Manager virtual appliance and select **Edit Settings**.
- 2 Select the **Options** tab.
- 3 Under **vApp Options**, click **Advanced**.
- 4 In the Properties section on the right, click the **Properties** button.
- 5 In the Advanced Property Configuration dialog box, configure the following keys:
  - vami.DNS.WorkspacePortal
  - vami.netmask0.WorkspacePortal
  - vami.gateway.WorkspacePortal
  - a Select one of the keys and click **Edit**.
  - b In the Edit Property Settings dialog box, next to the **Type** field, click **Edit**.
  - c In the Edit Property Type dialog box, select **Dynamic Property** and select the appropriate value from the drop down menu for **Netmask**, **Gateway Address**, and **DNS Servers** respectively.
  - d Click **OK**, and click **OK** again.
  - e Repeat these steps to configure each key.
- 6 Power on the virtual appliance.

The properties are configured to use IP Pools.

### What to do next

Configure VMware Identity Manager settings.

## Configure VMware Identity Manager Settings

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

### Prerequisites

- The VMware Identity Manager virtual appliance is powered on.
- If you are using an external database, the external database is configured and the external database connection information is available. See [“Connecting to the Database,”](#) on page 28 for information.

- Review [Chapter 4, “Integrating with Active Directory,”](#) on page 39 for information about the Active Directory configuration.
- You have your Active Directory information.
- When multi-forest Active Directory is configured and the Domain Local group contains members from domains in different forests, the Bind DN user used on the VMware Identity Manager Directory page must be added to the Administrators group of the domain in which Domain Local group resides. If this is not done, these members will be missing from the Domain Local group.
- You have a list of the Active Directory user attributes you want to use as filters, and a list of the groups you want to add to VMware Identity Manager.

**Procedure**

- 1 Go to the VMware Identity Manager URL that is shown on the blue screen in the **Console** tab. For example, `https://hostname.example.com`.
- 2 Accept the certificate, if prompted.
- 3 In the Get Started page, click **Continue**.
- 4 In the Set Passwords page, set passwords for the following administrator accounts, which are used to manage the appliance, then click **Continue**.

---

**Account**

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

- 5 In the Select Database page, select the database to use.  
See [“Connecting to the Database,”](#) on page 28 for more information.
  - If you are using an external database, select **External Database** and enter the external database connection information, user name, and password. To verify that VMware Identity Manager can connect to the database, click **Test Connection**.  
After you verify the connection, click **Continue**.
  - If you are using the internal database, click **Continue**.

The connection to the database is configured and the database is initialized. When the process is complete, the **Setup is complete** page appears.
- 6 Click the **Log in to the administration console** link on the **Setup is complete** page to log in to the administration console to set up the Active Directory connection.
- 7 Log in to the administration console as the **admin** user, using the password you set.  
You are logged in as a Local Admin. The Directories page appears. Before you add a directory, ensure that you review the [Chapter 4, “Integrating with Active Directory,”](#) on page 39 for information about Active Directory environments and requirements.
- 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. 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.

---

---

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

---

- 10 Click **Save**.
- 11 Click the **Identity & Access Management** tab, and, in the Directories page, click **Add Directory**.
- 12 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)**.

## 13 Configure the connection information.

Option	Description
<b>Active Directory over LDAP</b>	<p data-bbox="711 275 1393 352">a In the <b>Sync Connector</b> field, select the connector you want to use to sync users and groups from Active Directory to the VMware Identity Manager directory.</p> <p data-bbox="748 369 1410 499">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.</p> <p data-bbox="711 506 1414 558">b In the <b>Authentication</b> field, if you want to use this Active Directory to authenticate users, click <b>Yes</b>.</p> <p data-bbox="748 575 1425 705">If you want to use a third-party identity provider to authenticate users, click <b>No</b>. After you configure the Active Directory connection to sync users and groups, go to the <b>Identity &amp; Access Management &gt; Manage &gt; Identity Providers</b> page to add the third-party identity provider for authentication.</p> <p data-bbox="711 716 1425 768">c In the <b>Directory Search Attribute</b> field, select the account attribute that contains username.</p> <p data-bbox="711 779 1393 831">d If the Active Directory uses DNS Service Location lookup, make the following selections.</p> <ul style="list-style-type: none"> <li data-bbox="748 835 1414 888">■ In the <b>Server Location</b> section, select the <b>This Directory supports DNS Service Location</b> checkbox.</li> </ul> <p data-bbox="785 905 1406 1003">A <code>domain_krb.properties</code> file, auto-populated with a list of domain controllers, will be created when the directory is created. See <a href="#">“About Domain Controller Selection (domain_krb.properties file),”</a> on page 42 .</p> <ul style="list-style-type: none"> <li data-bbox="748 1014 1406 1113">■ If the Active Directory requires STARTTLS encryption, select the <b>This Directory requires all connections to use SSL</b> check box in the <b>Certificates</b> section and copy and paste the Active Directory Root CA certificate into the <b>SSL Certificate</b> field.</li> </ul> <p data-bbox="785 1136 1390 1188">Ensure the certificate is in PEM format and include the "BEGIN CERTIFICATE" and "END CERTIFICATE" lines.</p> <p data-bbox="785 1192 1414 1245"><b>NOTE</b> If the Active Directory requires STARTTLS and you do not provide the certificate, you cannot create the directory.</p> <p data-bbox="711 1255 1377 1308">e If the Active Directory does not use DNS Service Location lookup, make the following selections.</p> <ul style="list-style-type: none"> <li data-bbox="748 1312 1425 1390">■ In the <b>Server Location</b> section, verify that the <b>This Directory supports DNS Service Location</b> checkbox is not selected and enter the Active Directory server host name and port number.</li> </ul> <p data-bbox="785 1409 1390 1486">To configure the directory as a global catalog, see the Multi-Domain, Single Forest Active Directory Environment section in <a href="#">“Active Directory Environments,”</a> on page 40.</p> <ul style="list-style-type: none"> <li data-bbox="748 1497 1414 1596">■ If the Active Directory requires access over SSL, select the <b>This Directory requires all connections to use SSL</b> check box in the <b>Certificates</b> section and copy and paste the Active Directory Root CA certificate into the <b>SSL Certificate</b> field.</li> </ul>

Option	Description
	<p>Ensure the certificate is in PEM format and include the "BEGIN CERTIFICATE" and "END CERTIFICATE" lines.</p> <p><b>NOTE</b> If the Active Directory requires SSL and you do not provide the certificate, you cannot create the directory.</p> <p>f In the <b>Base DN</b> field, enter the DN from which to start account searches. For example, OU=myUnit,DC=myCorp,DC=com.</p> <p>g In the <b>Bind DN</b> field, enter the account that can search for users. For example, CN=binduser,OU=myUnit,DC=myCorp,DC=com.</p> <p>h After you enter the Bind password, click <b>Test Connection</b> to verify that the directory can connect to your Active Directory.</p>
<b>Active Directory (Integrated Windows Authentication)</b>	<p>a In the <b>Sync Connector</b> field, select the connector you want to use to sync users and groups from Active Directory to the VMware Identity Manager directory.</p> <p>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.</p> <p>b In the <b>Authentication</b> field, if you want to use this Active Directory to authenticate users, click <b>Yes</b>.</p> <p>If you want to use a third-party identity provider to authenticate users, click <b>No</b>. After you configure the Active Directory connection to sync users and groups, go to the <b>Identity &amp; Access Management &gt; Manage &gt; Identity Providers</b> page to add the third-party identity provider for authentication.</p> <p>c In the <b>Directory Search Attribute</b> field, select the account attribute that contains username.</p> <p>d If the Active Directory requires STARTTLS encryption, select the <b>This Directory requires all connections to use STARTTLS</b> checkbox in the <b>Certificates</b> section and copy and paste the Active Directory Root CA certificate into the <b>SSL Certificate</b> field.</p> <p>Ensure the certificate is in PEM format and include the "BEGIN CERTIFICATE" and "END CERTIFICATE" lines.</p> <p>If the directory has multiple domains, add the Root CA certificates for all domains, one at a time.</p> <p><b>NOTE</b> If the Active Directory requires STARTTLS and you do not provide the certificate, you cannot create the directory.</p> <p>e Enter the name of the Active Directory domain to join. Enter a user name and password that has the rights to join the domain. See <a href="#">"Joining a Domain,"</a> on page 47 for more information.</p> <p>f In the <b>Bind User UPN</b> field, enter the User Principal Name of the user who can authenticate with the domain. For example, username@example.com.</p> <p>g Enter the Bind DN User password.</p>

14 Click **Save & Next**.

The page with the list of domains appears.

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

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

---

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

---

Click **Next**.

- 16 Verify that the VMware Identity Manager directory attribute names are mapped to the correct Active Directory attributes. If not, select the correct Active Directory attribute from the drop-down list. Click **Next**.
- 17 Click + to select the groups you want to sync from Active Directory to the VMware Identity Manager directory.

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

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

---

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

---

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

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

Click **Next**.

- 20 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.

- 21 Click **Sync Directory** to start the directory sync.

---

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

---

### What to do next

For information about setting up a load balancer or a high-availability configuration, see [Chapter 5, "Advanced Configuration for the VMware Identity Manager Appliance,"](#) on page 53.

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



## Setting Proxy Server Settings for VMware Identity Manager

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

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

---

**NOTE** Proxy servers that require authentication are not supported.

---

### Procedure

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

```
service horizon-workspace restart
```

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

## Enter the License Key

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

### Procedure

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



# Managing Appliance System Configuration Settings

# 3

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

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

Page Name	Setting Description
Database Connection	The database connection setting, either Internal or External, is enabled. You can change the database type. When you select External Database, you enter the external database URL, user name, and password. To set up an external database, see <a href="#">“Connecting to the Database,”</a> on page 28.
Install Certificate	On this page, you install a custom or self-signed certificate for VMware Identity Manager and, if VMware Identity Manager is configured with a load balancer, you can install the load balancer's root certificate. The location of the VMware Identity Manager root CA certificate is displayed on this page as well, on the <a href="#">Terminate SSL on a Load Balancer</a> tab. See <a href="#">“Using SSL Certificates,”</a> on page 33.
Identity Manager FQDN	The VMware Identity Manager FQDN is displayed on this page. You can change it. VMware Identity Manager FQDN is the URL that users use to access the service.
Configure Syslog	On this page, you can enable an external syslog server. VMware Identity Manager logs are sent to this external server. See <a href="#">“Enable the Syslog Server,”</a> on page 36.
Change Password	On this page, you can change the VMware Identity Manager admin user password.
System Security	On this page, you can change the root password for the VMware Identity Manager appliance and the ssh user password used to log in remotely.
Log File Locations	A list of log files and their directory locations is displayed on this page. You can bundle the log files into a tar zip file and download it. See <a href="#">“Log File Information,”</a> on page 37.

You can also modify the connector URL. See [“Modifying the Connector URL,”](#) on page 36.

This chapter includes the following topics:

- [“Change Appliance Configuration Settings,”](#) on page 28
- [“Connecting to the Database,”](#) on page 28
- [“Using SSL Certificates,”](#) on page 33

- “Modifying the VMware Identity Manager Service URL,” on page 35
- “Modifying the Connector URL,” on page 36
- “Enable the Syslog Server,” on page 36
- “Log File Information,” on page 37
- “Manage Your Appliance Passwords,” on page 38
- “Configure SMTP Settings,” on page 38

## Change Appliance Configuration Settings

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

### Procedure

- 1 Log in to the administration console.
- 2 Select the **Appliance Settings** tab and click **Manage Configuration**.
- 3 Log in with the service administrator password.
- 4 In the left pane, select the page to view or edit.

### What to do next

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

## Connecting to the Database

An internal PostgreSQL database is embedded in the VMware Identity Manager appliance. To use an external database with VMware Identity Manager, your database administrator must prepare an empty database and schema before connecting to the database in VMware Identity Manager.

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

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

Existing users who are using an external vPostgres database can continue to use that database when they upgrade to this release

---

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

---

## Configure a Microsoft SQL Database

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

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

---

**NOTE** The default collation should be case-sensitive.

---

### Prerequisites

- Supported version of the Microsoft SQL server installed as an external database server. See the VMware Product Interoperability Matrixes at [http://www.vmware.com/resources/compatibility/sim/interop\\_matrix.php](http://www.vmware.com/resources/compatibility/sim/interop_matrix.php).

- Administrator rights to access and create the database components using Microsoft SQL Server Management Studio or from another Microsoft SQL Server CLI client.

### Procedure

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

The editor window appears.

- 2 In the toolbar click **New Query**.
- 3 Cut and paste the following commands in to the editor window.

---

#### Microsoft SQL Commands

---

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

---

Note that the CREATE LOGIN command creates the user named horizon with the password H0rizon!

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

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

### What to do next

Configure the external database on the VMware Identity Manager server. Go to the VMware Identity Manager administration console Appliance Settings > VA Configuration > Database Connection Setup page. Enter the JDBC URL as jdbc:sqlserver://<DB\_VM\_IP\_ADDR>;DatabaseName=saas. Enter the user name and password created for the database. See [“Add an External Database to the VMware Identity Manager Appliance,”](#) on page 32

## Configure an Oracle Database

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

### Prerequisites

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

**Procedure**

- 1 Specify the following settings when creating an Oracle database.
  - a Select the **General Purpose/Transaction Processing Database** configuration option.
  - b Click **Use Unicode > UTF8**.
  - c Use National Character Set.
- 2 Connect to the Oracle database after the installation is finished.
- 3 Log in to the Oracle database as the sys user.
- 4 Increase the process connections. Each additional service virtual machine requires a minimum of 300 process connections to function with VMware Identity Manager. For example, if your environment has two service virtual machines, run the `alter` command as sys or system user.
  - a Increase the process connections using the `alter` command.
 

```
alter system set processes=600 scope=spfile
```
  - b Restart the database.
- 5 Create a database trigger that all users can use.

---

**Sample SQL to Create a Database Trigger**

---

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

---

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

---

**Sample SQL to Create a New User**

---

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

---

## Configure a PostgreSQL Database

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

---

**NOTE** VMware Identity Manager does not currently support generic PostgreSQL.

---

### Prerequisites

- Install and configure a supported version of VMware vFabric PostgreSQL as the external database server from one of the installation packages, such as OVA, OVF, or RPM, with the citext module installed. The citext module supports the CITEXT data type, a case insensitive text type. Verify that the VMware vFabric PostgreSQL version that you use is compatible with your version of VMware Identity Manager. For information about supported VMware vFabric PostgreSQL versions, see the VMware Product Interoperability Matrixes at [http://www.vmware.com/resources/compatibility/sim/interop\\_matrix.php](http://www.vmware.com/resources/compatibility/sim/interop_matrix.php).
- Install and configure the load balancing implementation.
- Verify that your environment meets these requirements:
  - The database server you use is PostgreSQL.
  - The database administrator username and password are available.
  - You must enter a username and password to create a user with authorization to the *saas* schema. This user is required when you connect a VMware Identity Manager virtual machine instance to the database.

---

**NOTE** The VMware Identity Manager virtual machine uses the database name *saas*. During the initialization process, it drops and recreates any existing database named *saas*.

---

### Procedure

- 1 Log in as the root user.
- 2 Edit the `postgresql.conf` file.  
 For example, the VMware vFabric PostgreSQL database location is `/var/vmware/vpostgres/current/pgdata/`.
- 3 Increase the `max_connections` parameter. Each additional VMware Identity Manager virtual machine requires at least 300 connections to function properly with VMware Identity Manager.
- 4 Set the `max_connections` parameter value to **600** for the two VMware Identity Manager virtual machines.
- 5 Restart the database.
- 6 Add a new line to the `postgresql.conf.auto` file that includes the `search_path='saas'` parameter.

- 7 Run the PostgreSQL commands to create a new PostgreSQL database schema.

**Table 3-1. Create a New Database Schema SQL**

---

**Sample SQL to Create a New Database Schema**

---

```
CREATE ROLE horizon LOGIN
PASSWORD yourpassword
NOSUPERUSER INHERIT NOCREATEDB NOCREATEROLE NOREPLICATION;
ALTER ROLE horizon
SET search_path = saas;
CREATE DATABASE saas
WITH OWNER = postgres
ENCODING = 'UTF8'
TABLESPACE = pg_default
CONNECTION LIMIT = -1;
GRANT CONNECT, TEMPORARY ON DATABASE saas TO public;
GRANT ALL ON DATABASE saas TO postgres;
GRANT ALL ON DATABASE saas TO horizon;
\connect saas;
CREATE SCHEMA saas AUTHORIZATION horizon;
CREATE EXTENSION citext SCHEMA saas;
```

---

## Transfer Data from the Internal Database

If your deployment uses an internal database and you plan to switch to an external database, you can extract the existing data from the database and add it to a new external database.

### Prerequisites

Prepare the external database server. See [“Configure a PostgreSQL Database,”](#) on page 31.

### Procedure

- 1 Log in as the root user.
- 2 Go to the `/opt/vmware/vpostgres/current/bin` directory.
- 3 Run the `./pg_dump -U postgres -w --clean -f /tmp/db_dump.data saas` command.
- 4 Copy the `db_dump.data` file to the newly prepared external database server.

```
scp /tmp/db_dump.data
```

- 5 Log in as the root user on the external database server.
- 6 Go to the `/opt/vmware/vpostgres/current/bin` directory.
- 7 Run the `db_dump.data` command.

```
./psql -U postgres -w -d saas -f /tmp/db_dump.data
```

You might see DROP and ALTER commands while the `db_dump.data` command runs.

## Add an External Database to the VMware Identity Manager Appliance

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

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



### Prerequisites

- Install and configure the supported Microsoft SQL, Oracle edition, or VMware vFabric PostgreSQL as the external database server. For information about specific versions that are supported by VMware Identity Manager, see the VMware Product Interoperability Matrixes at [http://www.vmware.com/resources/compatibility/sim/interop\\_matrix.php](http://www.vmware.com/resources/compatibility/sim/interop_matrix.php).
- Transfer data from the internal database, if you had been using one.

### Procedure

- 1 In the administration console click **Appliance Settings** and select **VA Configuration**.
- 2 Click **Manage Configuration**.
- 3 Log in with the VMware Identity Manager administrator password.
- 4 On the Database Connection Setup page, select **External Database** as the database type.
- 5 Enter information about the database connection.
  - a Type the JDBC URL of the database server.

**PostgreSQL**                      `jdbc:postgresql://IP_address/saas?stringtype=unspecified`

**Microsoft SQL**                      `jdbc:sqlserver://IP_address;DatabaseName=saas`

**Oracle**                              `jdbc:oracle:thin:@//IP_address:port/sid`

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

**PostgreSQL**                      horizon

**Microsoft SQL**                      horizon

**Oracle**                              "saas"

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

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

## Using SSL Certificates

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

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

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

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

## Apply Public Certificate Authority

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

---

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

---

### Prerequisites

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

### Procedure

- 1 In the administration console, click **Appliance Settings**.  
VA configuration is selected by default.
- 2 Click **Manage Configuration**.
- 3 In the dialog box that appears, enter the VMware Identity Manager server admin user password.
- 4 Select **Install Certificate**.
- 5 In the Terminate SSL on Identity Manager Appliance tab, select **Custom Certificate**.
- 6 In the **SSL Certificate Chain** text box, paste the host, intermediate, and root certificates, in that order.  
  
The SSL certificate works only if you include the entire certificate chain in the correct order. For each certificate, copy everything between and including the lines -----BEGIN CERTIFICATE----- and -----END CERTIFICATE-----  
  
Ensure that the certificate includes the FQDN hostname.
- 7 Paste the private key in the Private Key text box. Copy everything between ----BEGIN RSA PRIVATE KEY and ---END RSA PRIVATE KEY.
- 8 Click **Save**.

### Example: Certificate Examples

---

#### Certificate Chain Example

---

```
-----BEGIN CERTIFICATE-----
jIQvt9WdR9Vpg3WQT5+C3HU17bUOwvhp/r0+
...
...
...
W53+O05j5xsxzDJfWr11qB1FF/OkIYCPcyK1
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
WdR9Vpg3WQT5+C3HU17bUOwvhp/rjIQvt90+
...
...
...
O05j5xsxzDJfWr11qB1FF/OkIYCPW53+cyK1
-----END CERTIFICATE-----
```

---

---

**Certificate Chain Example**

---

```

-----BEGIN CERTIFICATE-----
dR9Vpg3WQTjIQvt9W5+C3HU17bUOwvhp/r0+
...
...
5j5xsxzDJfWr1lqW53+O0BIFF/OkIYCPcyK1
-----END CERTIFICATE-----

```

---

**Private Key Example**

---

```

-----BEGIN RSA PRIVATE KEY-----
jIQvtg3WQT5+C3HU17bU9WdR9VpOwvhp/r0+
...
...
1lqBIFFW53+O05j5xsxzDJfWr/OkIYCPcyK1
-----END RSA PRIVATE KEY-----

```

---

## Adding SSL Certificates

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

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

---

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

---



---

**Certificate Chain Example**

---

```

-----BEGIN CERTIFICATE-----
SSL Cert - Appliance SSL Cert
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
Intermediate/Issuing CA Cert
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
Root CA Cert
-----END CERTIFICATE-----

```

---

## Modifying the VMware Identity Manager Service URL

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

**Procedure**

- 1 Log into the VMware Identity Manager administration console.
- 2 Click the **Appliance Settings** tab, then select **VA Configuration**.

- 3 Click **Manage Configuration** and log in with the **admin** user password.
- 4 Click **Identity Manager FQDN** and enter the new URL in the **Identity Manager FQDN** field.  
Use the format **https://FQDN:port**. Specifying a port is optional. The default port is 443.  
For example, **https://myservice.example.com**.
- 5 Click **Save**.

#### What to do next

Enable the new portal user interface.

- 1 Go to **https://VMwareIdentityManagerURL/admin** to access the administration console.
- 2 In the administration console, click the arrow on the **Catalog** tab and select **Settings**.
- 3 Select **New End User Portal UI** in the left pane and click **Enable New Portal UI**.

## Modifying the Connector URL

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

#### Procedure

- 1 Log in to the VMware Identity Manager administration console.
- 2 Click the **Identity & Access Management** tab, then click the **Identity Providers** tab.
- 3 In the Identity Providers page, select the identity provider to update.
- 4 In the **IdP Hostname** field, enter the new hostname.  
Use the format **hostname:port**. Specifying a port is optional. The default port is 443.  
For example, **vidm.example.com**.
- 5 Click **Save**.

## Enable the Syslog Server

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

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

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

#### Prerequisites

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

#### Procedure

- 1 Log in to the administration console.
- 2 Select the **Appliance Settings** tab and click **Manage Configuration**.
- 3 Click **Configure Syslog**.

- 4 Click **Enable**.
- 5 Enter the IP address or the FQDN of the server where you want to store the logs.
- 6 Click **Save**.

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

## Log File Information

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

**Table 3-2.** Log Files

Component	Location of Log File	Description
Identity Manager Service Logs	<code>/opt/vmware/horizon/workspace/logs/horizon.log</code>	Information about activity on the VMware Identity Manager application, such as entitlements, users, and groups.
Configurator Logs	<code>/opt/vmware/horizon/workspace/logs/configurator.log</code>	Requests that the Configurator receives from the REST client and the Web interface.
Connector Logs	<code>/opt/vmware/horizon/workspace/logs/connector.log</code>	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.
Update Logs	<code>/opt/vmware/var/log/update.log</code> <code>/opt/vmware/var/log/vami</code>	A record of output messages related to update requests during an upgrade of VMware Identity Manager.  The files in the <code>/opt/vmware/var/log/vami</code> directory are useful for troubleshooting. You can find these files on all virtual machines after an upgrade.
Apache Tomcat Logs	<code>/opt/vmware/horizon/workspace/logs/catalina.log</code>	Apache Tomcat records of messages that are not recorded in other log files.

## Collect Log Information

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

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

### Procedure

- 1 Log in to the administration console.
- 2 Select the **Appliance Settings** tab and click **Manage Configuration**.
- 3 Click **Log File Locations** and click **Prepare log bundle**.  
The information is collected into a tar.gz file that can be downloaded.
- 4 Download the prepared bundle.

### What to do next

To collect all logs, do this on each appliance.

## Manage Your Appliance Passwords

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

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

### Procedure

- 1 In the administration console, click the **Appliance Settings** tab.
- 2 Click **VA Configuration > Manage Configuration**.
- 3 To change the admin password, select **Change Password**. To change the root or sshuser passwords, select **System Security**.

---

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

---

- 4 Enter the new password.
- 5 Click **Save**.

## Configure SMTP Settings

You can configure SMTP server settings in VMware Identity Manager.

### Procedure

- 1 Log in to the administration console.
- 2 Select the **Appliance Settings** tab and click **SMTP**.
- 3 Enter the SMTP server host name.  
For example: smtp.example.com
- 4 Enter the SMTP server port number.  
For example: 25
- 5 (Optional) Enter a user name and password, if the SMTP server requires authentication.
- 6 Click **Save**.

# Integrating with Active Directory

---

During configuration, you establish a connection between VMware Identity Manager and your Active Directory deployment.

You can update your Active Directory configuration information in the administration console, by clicking the **Identity & Access Management** tab.

This chapter includes the following topics:

- [“Important Concepts Related to Active Directory,”](#) on page 39
- [“Active Directory Environments,”](#) on page 40
- [“About Domain Controller Selection \(domain\\_krb.properties file\),”](#) on page 42
- [“Managing User Attributes that Sync from Active Directory,”](#) on page 45
- [“Joining a Domain,”](#) on page 47
- [“Configure Active Directory Connection to the Service,”](#) on page 47

## Important Concepts Related to Active Directory

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

### Connector

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

- Syncs user and group data between Active Directory and the service.
- When being used as an identity provider, authenticates users to the service.

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

---

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

---

## Directory

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

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

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

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

## Worker

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

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

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

## Security Considerations

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

## Active Directory Environments

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

### Single Active Directory Domain Environment

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

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

For more information, see:

- [“About Domain Controller Selection \(domain\\_krb.properties file\),”](#) on page 42
- [“Managing User Attributes that Sync from Active Directory,”](#) on page 45



- [“Joining a Domain,”](#) on page 47
- [“Configure Active Directory Connection to the Service,”](#) on page 47

## Multi-Domain, Single Forest Active Directory Environment

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

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

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

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

For more information, see:

- [“About Domain Controller Selection \(domain\\_krb.properties file\),”](#) on page 42
  - [“Managing User Attributes that Sync from Active Directory,”](#) on page 45
  - [“Joining a Domain,”](#) on page 47
  - [“Configure Active Directory Connection to the Service,”](#) on page 47
- If Integrated Windows Authentication does not work in your Active Directory environment, create an Active Directory over LDAP directory type and select the global catalog option.

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

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

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

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

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

## Multi-Forest Active Directory Environment with Trust Relationships

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

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

For more information, see:

- [“About Domain Controller Selection \(domain\\_krb.properties file\),”](#) on page 42
- [“Managing User Attributes that Sync from Active Directory,”](#) on page 45
- [“Joining a Domain,”](#) on page 47
- [“Configure Active Directory Connection to the Service,”](#) on page 47

## Multi-Forest Active Directory Environment Without Trust Relationships

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

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

For more information, see:

- [“About Domain Controller Selection \(domain\\_krb.properties file\),”](#) on page 42
- [“Managing User Attributes that Sync from Active Directory,”](#) on page 45
- [“Joining a Domain,”](#) on page 47
- [“Configure Active Directory Connection to the Service,”](#) on page 47

## About Domain Controller Selection (domain\_krb.properties file)

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

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

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

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

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

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

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

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

Note that if an entry for a domain already exists in the file, it is not updated. For example, if you created a directory, then deleted it, the original domain entry remains in the file and is not updated.

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

For information on editing the `domain_krb.properties` file, see [“Editing the domain\\_krb.properties file,”](#) on page 44.

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

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

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

- The subnet of the connector must be present in the Active Directory configuration, or a subnet must be specified in the `runtime-config.properties` file. See [“Overriding the Default Subnet Selection,”](#) on page 44.

The subnet is used to determine the site.

- The Active Directory configuration must be site aware.

If the subnet cannot be determined or if your Active Directory configuration is not site aware, DNS Service Location lookup is used to find domain controllers, and the file is populated with a few domain controllers that are reachable. Note that these domain controllers may not be at the same geographical location as the connector, which can result in delays or timeouts while communicating with Active Directory. In this case, edit the `domain_krb.properties` file manually and specify the correct domain controllers to use for each domain. See [“Editing the domain\\_krb.properties file,”](#) on page 44.

## Sample domain\_krb.properties File

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

## Overriding the Default Subnet Selection

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

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

### Procedure

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

---

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

---

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

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

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

```
siteaware.subnet.override=10.100.0.0/20
```

- 3 Save and close the file.
- 4 Restart the service.

```
service horizon-workspace restart
```

## Editing the domain\_krb.properties file

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

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

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

See also [“About Domain Controller Selection \(domain\\_krb.properties file\),”](#) on page 42.

### Procedure

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

---

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

---

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

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

Use the following format:

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

For example:

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

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

---

**IMPORTANT** Domain names must be in lowercase.

---

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

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

- 5 Restart the service.

```
service horizon-workspace restart
```

## Troubleshooting domain\_krb.properties

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

### "Error resolving domain" error

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

### Domain controllers are unreachable

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

## Managing User Attributes that Sync from Active Directory

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

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

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

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

VMware Identity Manager Directory Attribute Name	Default Mapping to Active Directory Attribute
<code>userPrincipalName</code>	<code>userPrincipalName</code>
<code>distinguishedName</code>	<code>distinguishedName</code>
<code>employeeId</code>	<code>employeeID</code>

**Table 4-1.** Default Active Directory Attributes to Sync to Directory (Continued)

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

## Select Attributes to Sync with Directory

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

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

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

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

---

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

---

### Procedure

- 1 In the administration console, Identity & Access Management tab, click **Setup > User Attributes**.
- 2 In the Default Attributes section, review the required attribute list and make appropriate changes to reflect what attributes should be required.
- 3 In the Attributes section, add the VMware Identity Manager directory attribute name to the list.
- 4 Click **Save**.  
The default attribute status is updated and attributes you added are added on the directory's Mapped Attributes list.
- 5 After the directory is created, go to the **Manage > Directories** page and select the directory.
- 6 Click **Sync Settings > Mapped Attributes**.
- 7 In the drop-down menu for the attributes that you added, select the Active Directory attribute to map to.
- 8 Click **Save**.

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

## Joining a Domain

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

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

- Create Computer Objects
- Delete Computer Objects

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

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

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



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

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

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

## Configure Active Directory Connection to the Service

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

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

### Prerequisites

- Select the required default attributes and add additional attributes on the User Attributes page. See ["Select Attributes to Sync with Directory,"](#) on page 46.

---

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

---

- List of the Active Directory groups and users to sync from Active Directory.
- For Active Directory over LDAP, the information required includes the Base DN, Bind DN, and Bind DN password.
- For Active Directory Integrated Windows Authentication, the information required includes the domain's Bind user UPN address and password.
- If the Active Directory requires access over SSL or STARTTLS, the Root CA certificate of the Active Directory domain controller is required.

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

**Procedure**

- 1 In the administration console, click the **Identity & Access Management** tab.
- 2 On the Directories page, click **Add Directory**.
- 3 Enter a name for this VMware Identity Manager directory.



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

Option	Description
<b>Active Directory over LDAP</b>	<p>a In the <b>Sync Connector</b> field, select the connector to use to sync with Active Directory.</p> <p>b In the <b>Authentication</b> field, if this Active Directory is used to authenticate users, click <b>Yes</b>.</p> <p>If a third-party identity provider is used to authenticate users, click <b>No</b>. After you configure the Active Directory connection to sync users and groups, go to the Identity &amp; Access Management &gt; Manage &gt; Identity Providers page to add the third-party identity provider for authentication.</p> <p>c In the <b>Directory Search Attribute</b> field, select the account attribute that contains username.</p> <p>d If the Active Directory uses DNS Service Location lookup, make the following selections. <ul style="list-style-type: none"> <li>■ In the <b>Server Location</b> section, select the <b>This Directory supports DNS Service Location</b> checkbox. <p>A <code>domain_krb.properties</code> file, auto-populated with a list of domain controllers, will be created when the directory is created. See <a href="#">“About Domain Controller Selection (domain_krb.properties file),”</a> on page 42 .</p> </li> <li>■ If the Active Directory requires STARTTLS encryption, select the <b>This Directory requires all connections to use SSL</b> check box in the <b>Certificates</b> section and copy and paste the Active Directory Root CA certificate into the <b>SSL Certificate</b> field. <p>Ensure the certificate is in PEM format and include the "BEGIN CERTIFICATE" and "END CERTIFICATE" lines.</p> <p><b>NOTE</b> If the Active Directory requires STARTTLS and you do not provide the certificate, you cannot create the directory.</p> </li> </ul> </p> <p>e If the Active Directory does not use DNS Service Location lookup, make the following selections. <ul style="list-style-type: none"> <li>■ In the <b>Server Location</b> section, verify that the <b>This Directory supports DNS Service Location</b> checkbox is not selected and enter the Active Directory server host name and port number. <p>To configure the directory as a global catalog, see the Multi-Domain, Single Forest Active Directory Environment section in <a href="#">“Active Directory Environments,”</a> on page 40.</p> </li> <li>■ If the Active Directory requires access over SSL, select the <b>This Directory requires all connections to use SSL</b> check box in the <b>Certificates</b> section and copy and paste the Active Directory Root CA certificate into the <b>SSL Certificate</b> field. <p>Ensure the certificate is in PEM format and include the "BEGIN CERTIFICATE" and "END CERTIFICATE" lines.</p> <p><b>NOTE</b> If the Active Directory requires SSL and you do not provide the certificate, you cannot create the directory.</p> </li> </ul> </p> <p>f In the <b>Base DN</b> field, enter the DN from which to start account searches. For example, <code>OU=myUnit,DC=myCorp,DC=com</code>.</p> <p>g In the <b>Bind DN</b> field, enter the account that can search for users. For example, <code>CN=binduser,OU=myUnit,DC=myCorp,DC=com</code>.</p> <p>h After you enter the Bind password, click <b>Test Connection</b> to verify that the directory can connect to your Active Directory.</p>
<b>Active Directory (Integrated Windows Authentication)</b>	<p>a In the <b>Sync Connector</b> field, select the connector to use to sync with Active Directory .</p> <p>b In the <b>Authentication</b> field, if this Active Directory is used to authenticate users, click <b>Yes</b>.</p>

Option	Description
	<p>If a third-party identity provider is used to authenticate users, click <b>No</b>. After you configure the Active Directory connection to sync users and groups, go to the Identity &amp; Access Management &gt; Manage &gt; Identity Providers page to add the third-party identity provider for authentication.</p>
c	<p>In the <b>Directory Search Attribute</b> field, select the account attribute that contains username.</p>
d	<p>If the Active Directory requires STARTTLS encryption, select the <b>This Directory requires all connections to use STARTTLS</b> checkbox in the <b>Certificates</b> section and copy and paste the Active Directory Root CA certificate into the <b>SSL Certificate</b> field.</p>
	<p>Ensure the certificate is in PEM format and include the "BEGIN CERTIFICATE" and "END CERTIFICATE" lines.</p>
	<p>If the directory has multiple domains, add the Root CA certificates for all domains, one at a time.</p>
	<p><b>NOTE</b> If the Active Directory requires STARTTLS and you do not provide the certificate, you cannot create the directory.</p>
e	<p>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 <a href="#">"Joining a Domain,"</a> on page 47 for more information.</p>
f	<p>In the Bind User UPN field, enter the User Principal Name of the user who can authenticate with the domain. For example, username@example.com.</p>
g	<p>Enter the Bind User password.</p>

5 Click **Save & Next**.

The page with the list of domains appears.

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

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

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

Click **Next**.

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

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

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

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

---

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

---

- 9 Click **Next**.
- 10 Click **+** to add additional users. For example, enter as **CN=username,CN=Users,OU=myUnit,DC=myCorp,DC=com**.  
To exclude users, create a filter to exclude some types of users. You select the user attribute to filter by, the query rule, and the value.  
Click **Next**.
- 11 Review the page to see how many users and groups are syncing to the directory and to view the sync schedule.  
To make changes to users and groups, or to the sync frequency, click the **Edit** links.
- 12 Click **Sync Directory** to start the sync to the directory.

The connection to the Active Directory is complete and the users and groups you selected are added to the directory.

### What to do next

- If you created a directory that supports DNS Service Location, a `domain_krb.properties` file was created and auto-populated with a list of domain controllers. View the file to verify or edit the list of domain controllers. See [“About Domain Controller Selection \(domain\\_krb.properties file\),”](#) on page 42.
- Set up authentication methods. After users and groups sync to the directory, if the connector is also used for authentication, you can set up additional authentication methods on the connector. If a third party is the authentication identity provider, configure that identity provider in the connector.
- Review the default access policy. The default access policy is configured to allow all appliances in all network ranges to access the Web browser, with a session time out set to eight hours or to access a client app with a session time out of 2160 hours (90 days). You can change the default access policy and when you add Web applications to the catalog, you can create new ones.
- Apply custom branding to the administration console, user portal pages and the sign-in screen.



# Advanced Configuration for the VMware Identity Manager Appliance

---

# 5

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

The VMware Identity Manager architecture diagram demonstrates how you can deploy the VMware Identity Manager environment. See [Chapter 1, “Preparing to Install VMware Identity Manager,”](#) on page 7 for a typical deployment.

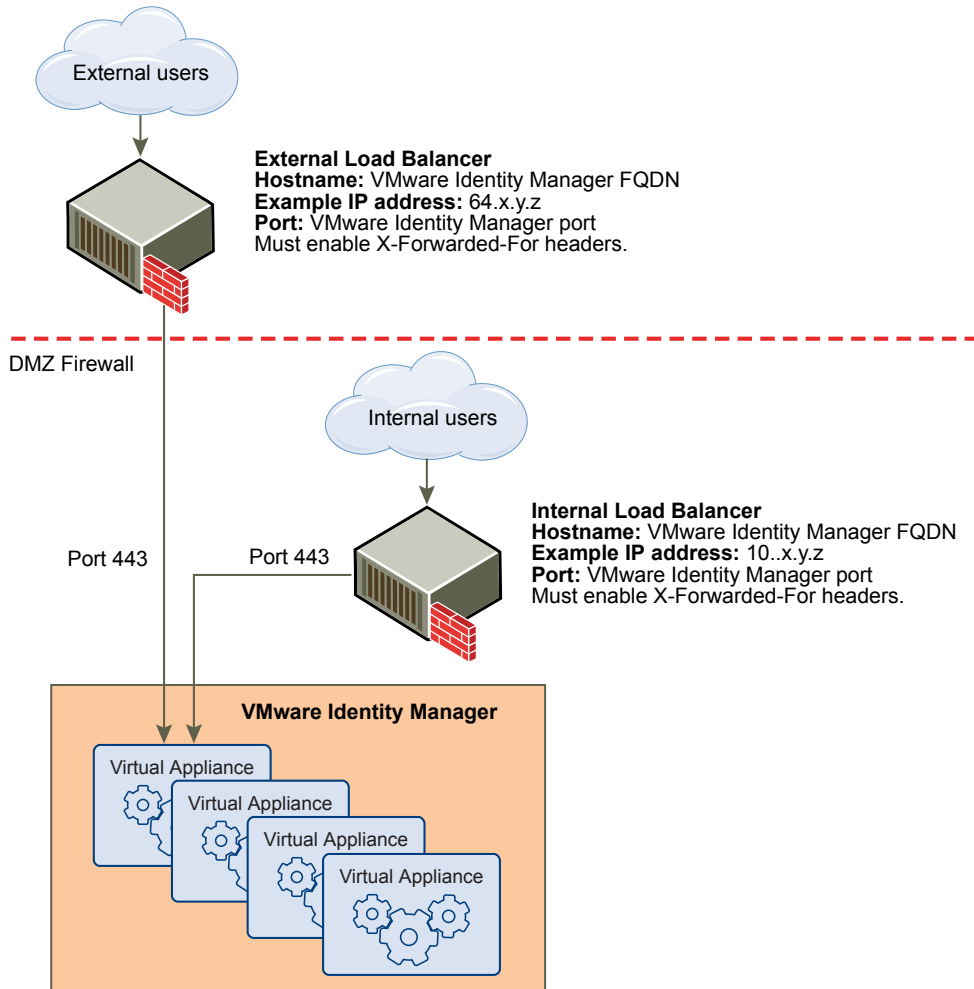
This chapter includes the following topics:

- [“Using a Load Balancer to Enable External Access to the VMware Identity Manager,”](#) on page 53
- [“Deploying Access Point for Reverse Proxy,”](#) on page 56
- [“Setting Proxy Server Settings for VMware Identity Manager,”](#) on page 57
- [“Configuring Redundancy,”](#) on page 57
- [“Deploying VMware Identity Manager in Secondary Data Center with Active-Active Read-Only Capability,”](#) on page 63

## Using a Load Balancer to Enable External Access to the VMware Identity Manager

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

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

**Figure 5-1.** External Load Balancer Proxy with Virtual Machine

## Specify VMware Identity Manager FQDN during Deployment

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

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

## Load Balancer Settings to Configure

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

- **X-Forwarded-For Headers.** You must enable X-Forwarded-For headers on your load balancer. This determines the authentication method. See the documentation provided by your load balancer vendor for more information.
- **Load Balancer Timeout.** For VMware Identity Manager to function correctly, you might need to increase the load balancer request timeout from the default. The value is set in minutes. If the timeout setting is too low, you might see this error, "502 error: The service is currently unavailable."

- Enabling Sticky Session on the Load Balancer to VMware Identity Manager. Ensure that you enable sticky session on the load balancer to the VMware Identity Manager appliances if your deployment uses multiple VMware Identity Manager appliances. Sticky session improves Web interface performance. If sticky session is not enabled, some functions might fail.

## Apply VMware Identity Manager Root Certificate to the Load Balancer

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

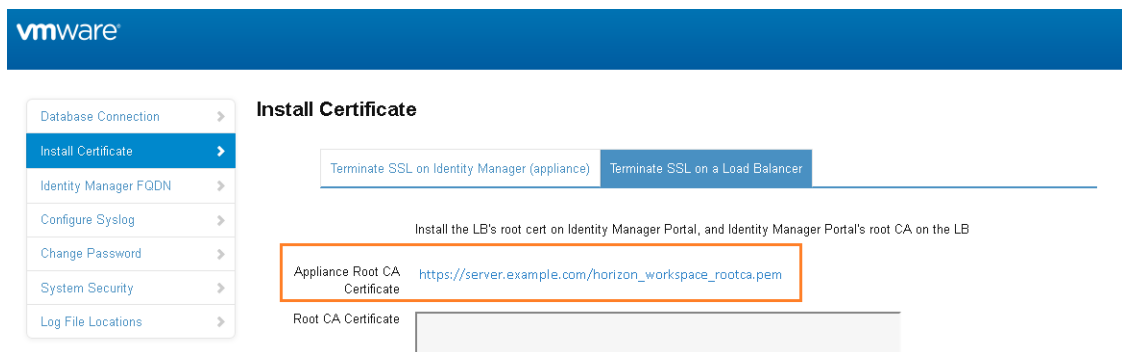
The VMware Identity Manager certificate can be downloaded from the administration console, from the **Appliance Settings > VA Configuration > Manage Configuration** page.

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

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

### Procedure

- 1 In the administration console, select the **Appliance Settings** tab and select **VA Configuration**.
- 2 Click **Manage Configuration**.
- 3 Select **Install Certificate**.
- 4 Select the **Terminate SSL on a Load Balancer** tab and in the **Appliance Root CA Certificate** field, click the link [https://hostname/horizon\\_workspace\\_rootca.pem](https://hostname/horizon_workspace_rootca.pem).



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

### What to do next

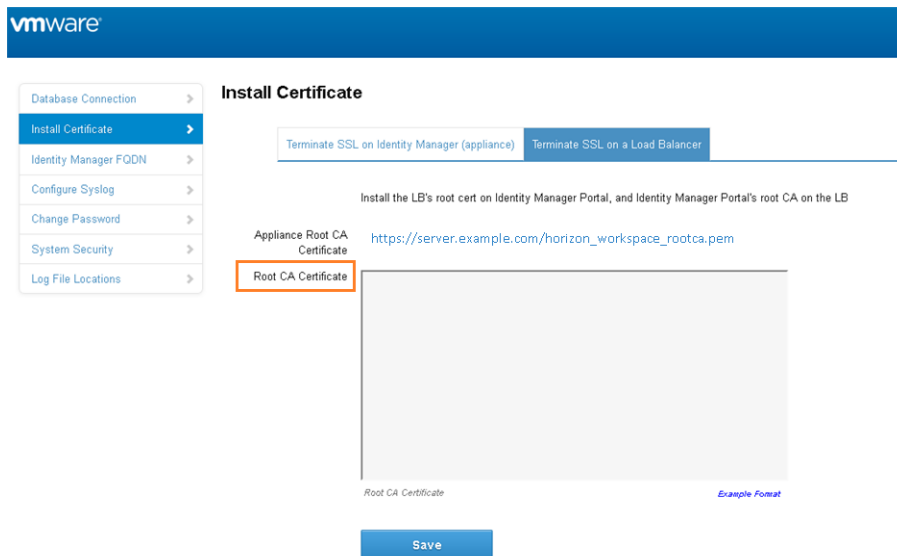
Copy and paste the load balancer root certificate to the VMware Identity Managerconnector appliance.

## Apply Load Balancer Root Certificate to VMware Identity Manager

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

### Procedure

- 1 Obtain the load balancer root certificate.
- 2 In the VMware Identity Manager administration console, select the **Appliance Settings** tab and select **VA Configuration**.
- 3 Click **Manage Configuration**.
- 4 Log in with the admin user password.
- 5 In the **Install Certificate** page, select the **Terminate SSL on a Load Balancer** tab.
- 6 Paste the text of the load balancer certificate into the **Root CA Certificate** field.



- 7 Click **Save**.

## Deploying Access Point for Reverse Proxy

With Access Point 2.6 and later releases, the Access Point appliance can serve as a reverse proxy for VMware Identity Manager.

An Access Point appliance resides within a DMZ behind the load balancers and in front of the VMware Identity Manager. Access Point acts as a reverse proxy to enable access to on-premises resources, including VMware Identity Manager, without the need of doing a VPN tunnel. Access Point also provides an additional level of abstraction and control to secure network traffic between clients and servers.

For information about deploying Access Point 2.6, see the Deploying and Configuring Access Point guide in the VMware Horizon 7 documentation center, <http://pubs.vmware.com/horizon-7-view/index.jsp>.



## Setting Proxy Server Settings for VMware Identity Manager

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

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

---

**NOTE** Proxy servers that require authentication are not supported.

---

### Procedure

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

```
service horizon-workspace restart
```

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

## Configuring Redundancy

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

You can also set up VMware Identity Manager in a secondary data center for failover and redundancy. If the primary VMware Identity Manager data center becomes unavailable, you redirect users to the secondary data center where they can continue to access resources in their My Apps portal.

### Configuring Failover and Redundancy

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

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

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

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

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

- 1 [Modify Internal Database](#) on page 58  
When you install and configure VMware Identity Manager, you select an external database or the internal database.
- 2 [Change VMware Identity Manager FQDN to Load Balancer FQDN](#) on page 58  
Before you clone the VMware Identity Manager virtual appliance, you must change its Fully Qualified Domain Name (FQDN) to match the load balancer FQDN.
- 3 [Clone the Virtual Appliance](#) on page 59
- 4 [Assign a New IP Address to Cloned Virtual Appliance](#) on page 60  
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.

## Modify Internal Database

When you install and configure VMware Identity Manager, you select an external database or the internal database.

If your VMware Identity Manager appliance is configured for an external database, you do not need to modify any settings before cloning the appliance. Cloned VMware Identity Manager virtual appliances will also use the external database that is configured for the original appliance.

If your VMware Identity Manager appliance is configured to use the internal database, you need to modify a few settings.

### Prerequisites

You have installed and configured a VMware Identity Manager virtual appliance and added it to a load balancer.

### Procedure

- ◆ (Internal database only) Follow the instructions in [VMware KB 2094258, Using embedded vPostgres in Production for VMware Workspace Portal VA 2.1](#).

## Change VMware Identity Manager FQDN to Load Balancer FQDN

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

### Prerequisites

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

### Procedure

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

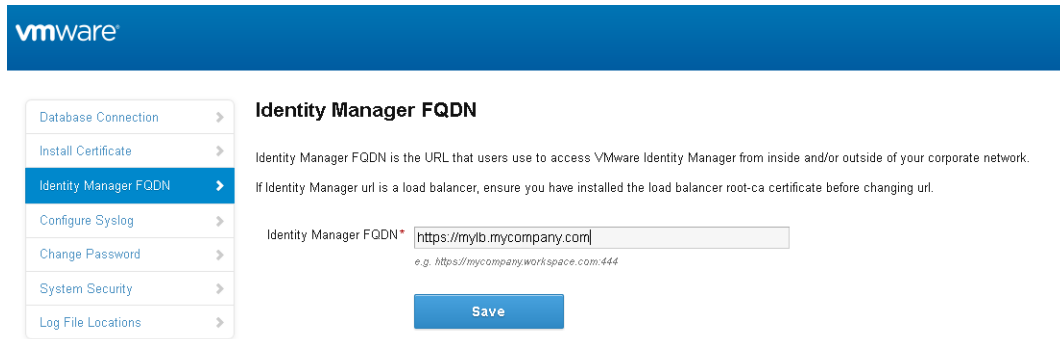
- 6 In the **Identity Manager FQDN** field, change the host name part of the URL from the VMware Identity Manager host name to the load balancer host name.

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

`https://myservice.mycompany.com`

to the following:

`https://mylb.mycompany.com`



- 7 Click **Save**.

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

### What to do next

Clone the virtual appliance.

### Clone the Virtual Appliance

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

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

### Prerequisites

- The VMware Identity Manager virtual appliance must be configured behind a load balancer. Make sure that the load balancer port is 443. Do not use 8443 as this port number is the administrative port and is unique to each virtual appliance.
- Either an external database configured as described in [“Connecting to the Database,”](#) on page 28 or an internal database configured as described in [VMware KB 2094258, Using embedded vPostgres in Production for VMware Workspace Portal VA 2.1](#), must be set up in order to add additional VMware Identity Manager virtual appliances.
- Ensure that you complete directory configuration in VMware Identity Manager.
- Log in to the virtual appliance console as root and delete the `/etc/udev/rules.d/70-persistent-net.rules` file, if it exists. If you do not delete this file before cloning, networking is not configured correctly on the cloned virtual appliance.

### Procedure

- 1 Log in to the vSphere Client or vSphere Web Client and navigate to the VMware Identity Manager virtual appliance.

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

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

#### What to do next

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

### Assign a New IP Address to Cloned Virtual Appliance

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

#### Procedure

- 1 In the vSphere Client or the vSphere Web Client, select the cloned virtual appliance.
- 2 In the **Summary** tab, under **Commands**, click **Edit Settings**.
- 3 Select **Options** and in the **vApp Options** list, select **Properties**.
- 4 Change the IP address in the **IP Address** field.
- 5 If the IP address is not in the reverse DNS, add the host name in the **HostName** text box.
- 6 Click **OK**.
- 7 Power on the cloned appliance and wait until the blue login screen appears in the **Console** tab.

---

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

---

#### What to do next

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

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

- a Log in to the cloned virtual appliance.
- b Check the Elasticsearch cluster:

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

Verify that the result matches the number of nodes.

- c Check the RabbitMQ cluster:

```
rabbitmqctl cluster_status
```

Verify that the result matches the number of nodes.

- Add the cloned virtual appliance to the load balancer and configure the load balancer to distribute traffic. See your load balancer vendor documentation for information.
- If you had joined a domain in the original service instance, then you need to join the domain in the cloned service instances.
  - a Log in to the VMware Identity Manager administration console.
  - b Select the **Identity & Access Management** tab, then click **Setup**.

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

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

For more information about Active Directory, see [Chapter 4, “Integrating with Active Directory,”](#) on page 39.

- For directories of type Integrated Windows Authentication (IWA), you must do the following:
  - a For the cloned service instances, join the domain to which the IWA directory in the original service instance was joined.
    - 1 Log in to the VMware Identity Manager administration console.
    - 2 Select the **Identity & Access Management** tab, then click **Setup**.

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

- 3 For each connector listed, click **Join Domain** and specify the domain information.
- b Save the IWA directory configuration.
    - 1 Select the **Identity & Access Management** tab.
    - 2 In the Directories page, click the IWA directory link.
    - 3 Click **Save** to save the directory configuration.

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

The VMware Identity Manager service virtual appliance is now highly available. Traffic is distributed to the virtual appliances in your cluster based on the load balancer configuration. Authentication to the service is highly available. For the directory sync feature of the service, however, in the event of a service instance failure, you will need to manually enable directory sync on a cloned service instance. Directory sync is handled by the connector component of the service and can only be enabled on one connector at a time. See [“Enabling Directory Sync on Another Instance in the Event of a Failure,”](#) on page 61

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

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

### Procedure

- 1 Log in to the VMware Identity Manager administration console.
- 2 Click the **Identity & Access Management** tab, then click **Directories**.

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

The screenshot shows the configuration page for a directory. At the top, there are tabs for 'Settings', 'Identity Providers', and 'Sync Log'. Under 'Directory Name', there is a text input field containing 'Example Directory' and two radio buttons: 'Active Directory over LDAP' (selected) and 'Active Directory (Integrated Windows Authentication)'. Below this is the 'Directory Sync and Authentication' section. It contains a heading 'Select the connector that syncs users from Active Directory to the VMware Identity Manager directory.' followed by a 'Sync Connector' dropdown menu with 'connector.example.com' selected. Below the dropdown are 'Identity Providers' (WorkspaceIDP\_\_1) and 'Directory Search Attribute' (sAMAccountName). A note at the bottom says 'Enter the account attribute that contains the user name.'

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

## Adding a Directory After Configuring Failover and Redundancy

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

You do this by adding the connector component of each of the service instances to the new directory.

### Procedure

- Log in to the VMware Identity Manager administration console.
- Select the **Identity & Access Management** tab, then select the **Identity Providers** tab.
- In the Identity Providers page, find the identity provider for the new directory and click the identity provider name.
- In the **IdP Hostname** field, enter the load balancer FQDN, if it is not already set to the correct load balancer FQDN.
- In the **Connector(s)** field, select the connector to add.
- Enter the password and click **Save**.
- In the Identity Providers page, click the Identity Provider name again and verify that the **IdP Hostname** field displays the correct host name. The **IdP Hostname** field should display the load balancer FQDN. If the name is incorrect, enter the load balancer FQDN and click **Save**.
- Repeat the preceding steps to add all the connectors listed in the **Connector(s)** field.

---

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

---

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

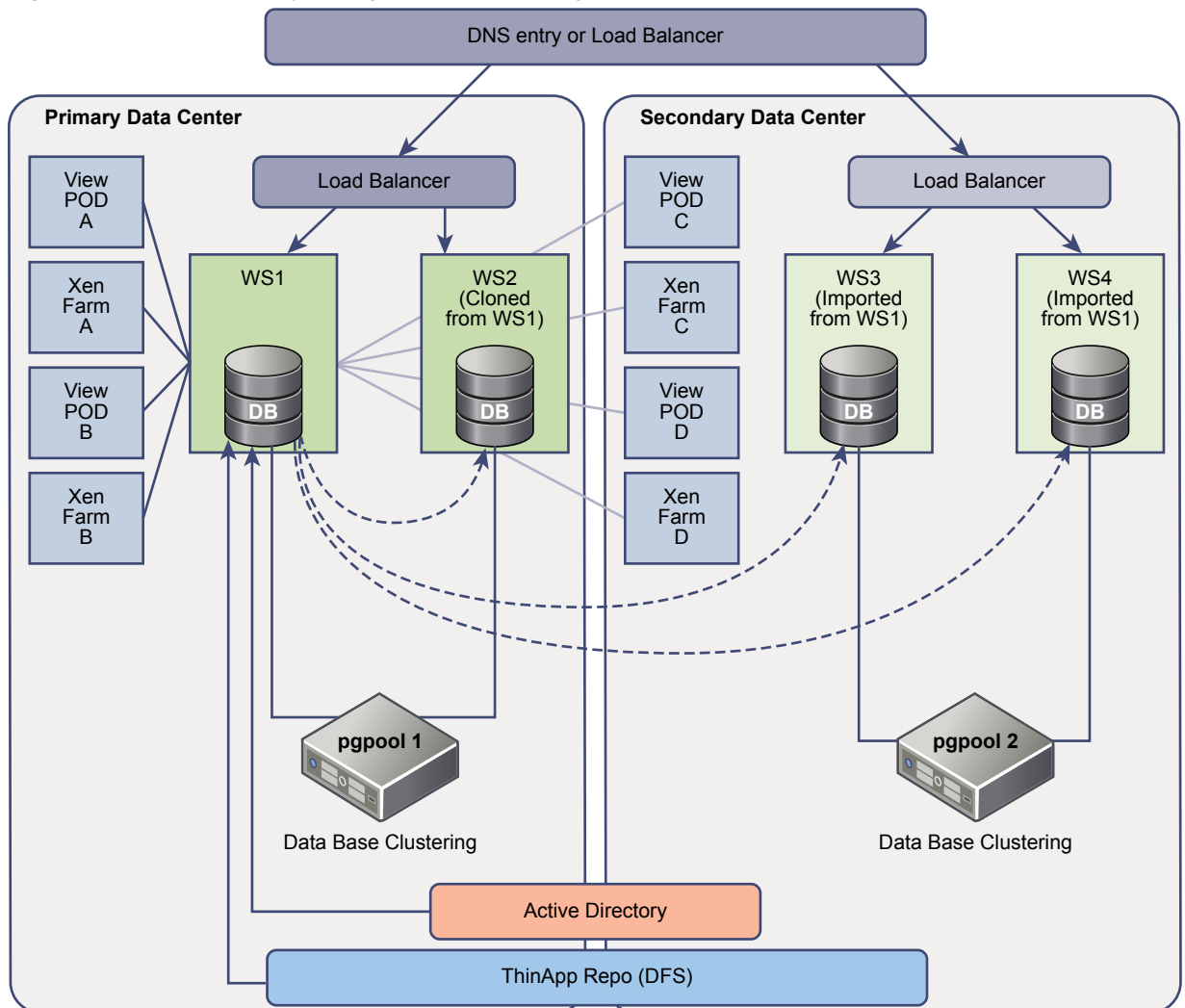
## Deploying VMware Identity Manager in Secondary Data Center with Active-Active Read-Only Capability

Deploy VMware Identity Manager in a secondary data center to provide failover capabilities if the primary VMware Identity Manager data center becomes unavailable.

Beginning with version 2.1.1, two options to provide failover capabilities to a secondary data center are available. The existing method of active - hot standby allows continuity of the entire VMware Identity Manager service with minimal downtime as the secondary data center is made primary. The method available beginning with version 2.1.1 enables a secondary data center to be powered on and active with read-only access, which eliminates any downtime during the fail-over. The read-only capability allows end users to view and launch their applications. This section documents how to set up a secondary data center in read-only mode.

**NOTE** If your enterprise environment requires second data center failover with full read/write capability, other deployment options are also available. See [KB 2094258, Using embedded vPostgres database for VMware Workspace Portal 2.1](#).

**Figure 5-2.** VMware Identity Manager Data Center Diagram



The scenario for Figure 1 is as follows:

- The primary data center includes WS1 as the master VMware Identity Manager server configured with an internal database. WS2 is cloned from WS1 and the database is configured as a slave to the master database in WS1.
- The secondary data center is a manual replication of the primary data center. The master VMware Identity Manager (WS1) configuration is imported to WS3 and WS4. The database is configured as slaves of WS1, with read-only access.
- Each data center is configured with a load balancer.
- The View Pods and Citrix-based Xen App Farm resources in the primary data center are setup in the secondary data center to mirror the configuration in the primary data center. When XenApp applications are configured, set up two Integration Brokers, one in each datacenter. Use a load balancer or a DNS record to control traffic flow to either the primary data center or to secondary data centers when the primary data center becomes unavailable. The ThinApp repository is set up in a Distributed File System (DFS) for high availability.
- The VMware Identity Manager FQDN should be served by a load balancer or a DNS entry which forwards all the traffic either to the load balancer in the primary data center or to the load balancer in the secondary data center.

## 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 servers in the secondary data center from the imported OVA file
- Load balancer for the secondary data center
- Duplicate View and Citrix-based desktops and applications and entitlements
- (Optional) pgpool-II for database redundancy to provide redundancy within a single datacenter
- Load balancer or DNS entry across the primary and secondary data centers for failover

## Add VMware Identity Manager Virtual Appliances by Importing OVA

To set up VMware Identity Manager in a second data center for redundancy, you export an OVA file of the primary VMware Identity Manager appliance and use the OVA file to deploy appliances in a secondary data center.

### Prerequisites

- VMware Identity Manager OVA file that was exported from the master VMware Identity Manager in the primary data center
- IP Address and DNS record of secondary data center

### Procedure

- 1 From the vSphere Client or the vSphere Web Client, select **Deploy OVF template** to deploy the VMware Identity Manager OVA file that was exported.
- 2 To install the appliances, see [“Install the VMware Identity Manager OVA File,”](#) on page 17.
- 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 master 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 master VMware Identity Manager appliance in the primary data center.
- In the Auth Adapters page, add the authentication methods that are configured in the primary data center.
- In the Directory Authentication Method page, enable Windows Authentication, if configured in the primary data center.

Go to the appliance settings Install Certificate page to add certificate authority signed certificates, duplicating the certificates in the VMware Identity Manager appliances in the primary data center. See [“Using SSL Certificates,”](#) on page 33.

**Edit runtime-config.properties File in Secondary Data Center**

You must edit the `runtime-config.properties` files for the VMware Identity Manager appliances in the secondary data center to change the JDBC URL to point to the database in the secondary data center and to configure the appliance for read-only access.

**Procedure**

- 1 Using a ssh client, log in to the VMware Identity Manager appliance as the root user.
- 2 Open the `runtime-config.properties` file at `/usr/local/horizon/conf/runtime-config.properties`.
- 3 Change the JDBC URL to point to the database for the secondary data center.  
See [“Add an External Database to the VMware Identity Manager Appliance,”](#) on page 32.
- 4 Configure the VMware Identity Manager appliance to have read-only access.  
Type `read.only.service=true`.
- 5 Restart the Tomcat server on the appliance.  
`service horizon-workspace restart`

**What to do next**

Repeat these steps on each VMware Identity Manager appliance in the secondary data center.

**Manage Resources Usage in Multiple VMware Identity Manager Data Centers**

You must configure the failover order of resources in both the primary and secondary data centers to make the appropriate resources available from any data center.

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

**Prerequisites**

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

**Procedure**

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

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

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

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

- For each service instance in your organization, configure the failover order for View and Citrix-based resources, type `hznAdminTool failoverConfiguration -configType <configType> -configuration <configuration> -serviceInstanceId <serviceInstanceId> [-orgId <orgId>]`

Option	Description
<b>-configType</b>	Type the resource type being configured for failover. Values are either VIEW or XENAPP.
<b>-configuration</b>	Type the failover order. For VIEW config type, type as a comma separated list of the primary View Connector Server host names that are listed in the View Pools page from the Connector Services Admin page. For XENAPP config type, type as a comma separated list of XenFarm names. XenFarm names are not displayed in the Workspace Connector Services Admin pages. Contact your XenApp administrator for the list of names.
<b>-serviceInstanceId</b>	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":
<b>-orgId</b>	(Optional). If left blank, the configuration is set for the default organization.

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

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

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

### What to do next

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

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

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

### Configure Database for Failover

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

Whether you are using the vPostgres internal database or configure an external database to work with VMware Identity Manager, you must configure your database for high availability. Configure a master and slave database architecture, where the slave is an exact replica of the master.

To set up your external database for high availability, refer to your external database documentation.

To set up the internal VMware Identity Manager database as a master and slave configuration for high availability, see [KB 2094258, Using embedded vPostgres database for VMware Workspace Portal 2.1](#).

## Using a DNS Record to Control Which Data Center is Active

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

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

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

### Setting Time To Live in DNS Record

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

## VMware Identity Manager Activities Not Available in Read-Only Mode

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

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

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

### VMware Identity Manager Administration Console Read-Only Mode

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

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

---

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

---

### **Appliance Configurator Pages Read-Only Mode**

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

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

### **End User My Apps Portal Read-Only Mode**

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

- Mark a resource as Favorite or unmark a resource as Favorite
- Drag and drop resources on the user's My Apps page to rearrange them
- Add resources from the App Center or remove resources from the user's My Apps page
- The label **New** is not removed from an application when it is launched

### **VMware Identity Manager Windows Client Read-Only Mode**

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

# Installing Additional Connector Appliances

---

# 6

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 Active 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.
- You want to use certificate-based authentication but your load balancer is configured to terminate SSL at the load balancer. Certificate authentication requires SSL pass-through at the load balancer.

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

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

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

This chapter includes the following topics:

- [“Generate Activation Code for Connector,”](#) on page 70
- [“Deploy the Connector OVA File,”](#) on page 70
- [“Configure Connector Settings,”](#) on page 71

## Generate Activation Code for Connector

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

### Procedure

- 1 Log in to the VMware Identity Manager administration console.
- 2 Click the **Identity & Access Management** tab.
- 3 Click **Setup**.
- 4 In the Connectors page, click **Add Connector**.
- 5 Enter a name for the new connector instance.
- 6 Click **Generate Activation Code**.

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

- 7 Copy and save the connector activation code.

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

### What to do next

Install the connector virtual appliance.

## Deploy the Connector OVA File

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

### Prerequisites

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

### Procedure

- 1 In the vSphere Client or the vSphere Web Client, select **File > Deploy OVF Template**.
- 2 In the Deploy OVF Template pages, enter the information specific to your deployment of the connector.

Page	Description
<b>Source</b>	Browse to the OVA package location, or enter a specific URL.
<b>OVA Template Details</b>	Verify that you selected the correct version.
<b>License</b>	Read the End User License Agreement and click <b>Accept</b> .
<b>Name and Location</b>	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.
<b>Host / Cluster</b>	Select the host or cluster to run the deployed template.
<b>Resource Pool</b>	Select the resource pool.
<b>Storage</b>	Select the location to store the virtual machine files.

Page	Description
<b>Disk Format</b>	Select the disk format for the files. For production environments, select a <b>Thick Provision</b> format. Use the <b>Thin Provision</b> format for evaluation and testing.
<b>Network Mapping</b>	Map the networks in your environment to the networks in the OVF template.
<b>Properties</b>	<ol style="list-style-type: none"> <li>In the <b>Timezone setting</b> field, select the correct time zone.</li> <li>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.</li> <li>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.</li> <li>To configure the static IP address for connector, enter the address for each of the following: Default Gateway, DNS, IP Address, and Netmask. <b>IMPORTANT</b> If any of the four address fields, including Host Name, are left blank, DHCP is used. To configure DHCP, leave the address fields blank.</li> </ol>
<b>Ready to Complete</b>	Review your selections and click <b>Finish</b> .

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

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

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

### What to do next

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

## Configure Connector Settings

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

### Prerequisites

- You have the activation code for the new connector. See [“Generate Activation Code for Connector,”](#) on page 70.
- 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

- To run the Setup wizard, enter the connector URL that was displayed in the Console tab after the OVA was deployed.
- 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
<b>Appliance Administrator</b>	Create the appliance administrator password. The user name is <b>admin</b> and cannot be changed. You use this account and password to log into the connector services to manage certificates, appliance passwords and syslog configuration. <b>IMPORTANT</b> The <b>admin</b> user password must be at least 6 characters in length.
<b>Root Account</b>	A default VMware root password was used to install the connector appliance. Create a new root password.
<b>sshuser Account</b>	Create the password to use for remote access to the connector appliance.

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

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

The connector configuration is complete.

#### What to do next

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

Configure SSL certificates for the connector. See [“Using SSL Certificates,”](#) on page 33.



# Preparing to Use Kerberos Authentication on iOS Devices

# 7

When you initially deploy the VMware Identity Manager service, your existing Active Directory infrastructure is used for user authentication and management. You integrate the service with other authentication solutions such as Kerberos, Certificate, and RSA SecurID from the administration console. To use Kerberos authentication for single sign-on to AirWatch managed iOS 9 devices requires you to manually initialize the Key Distribution Center (KDC) in the appliance before you can enable the built-in Kerberos authentication from the administration console.

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

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

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

This chapter includes the following topics:

- [“Pre- KDC Configuration Decisions,”](#) on page 73
- [“Initialize the Key Distribution Center in the Appliance,”](#) on page 74
- [“Creating Public DNS Entries for KDC with Built-in Kerberos,”](#) on page 75

## Pre- KDC Configuration Decisions

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

### Realm

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

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

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

## Using Subdomains

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

## Using KDC Server Certificates

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

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

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

## Initialize the Key Distribution Center in the Appliance

Before you can use the built-in Kerberos 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, it is recommended that you use descriptive names that end with your identity manager domain name. For example `SALES.MY-IDENTITYMANAGER.EXAMPLE.COM`. If you configure subdomains, type the subdomain name in lower-case letters.

### Prerequisites

VMware Identity Manager is installed and configured.

Realm name identified. See [“Pre- KDC Configuration Decisions,”](#) on page 73.

### Procedure

- 1 SSH into the VMware Identity Manager appliance as the root user.
- 2 Initialize the KDC. Enter `/etc/init.d/vmware-kdc init --realm {REALM.COM} --subdomain {sva-name.subdomain}`.

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

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

- 3 Restart the VMWare Identity Manager service. Enter `service horizon-workspace restart`.
- 4 Start the KDC service. Enter `service vmware-kdc restart`.

### What to do next

Create public DNS entries. DNS records must be provisioned to allow the clients to find the KDC. See [“Creating Public DNS Entries for KDC with Built-in Kerberos,”](#) on page 75.

## Creating Public DNS Entries for KDC with Built-in Kerberos

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

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

---

**NOTE** The AAAA entry value is an IPv6 address that encodes an IPv4 address. If the KDC is not addressable via IPv6 and an IPv4 address is used, the AAAA entry might have to be specified in 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 AAAA      ::ffff:1.2.3.4
kdc.example.com.           1800 IN A           1.2.3.4
_kerberos._tcp.EXAMPLE.COM      IN SRV 10 0    88 kdc.example.com.
```



# Index

## A

- Access Point **56**
- Access Point 2.6 **9**
- activation code **70**
- Active Directory Global Catalog **40**
- Active Directory
  - attribute mapping **46**
  - Integrated Windows Authentication **39**
  - integrating **40**
- Active Directory over LDAP **39, 47**
- add Active Directory **47**
- add certificates **34**
- additional connector **70**
- admin pages, appliance **27**
- admin console limitations in read only mode **67**
- appliance configurator, settings **28**
- appliance configuration **27**
- appliance configurator limitations in read-only mode **67**
- attributes
  - default **45**
  - mapping **46**

## C

- certificate authority **34**
- certificate chain **35**
- certificates, KDC **73**
- change
  - admin password **38**
  - root password **38**
  - sshuser password **38**
- checklist
  - Active Directory Domain Controller **13**
  - network information, IP Pools **13**
- cloned machines, adding IP address **60**
- collect logs **37**
- configuration settings, appliance **27**
- configure
  - logging **37**
  - virtual machines **53**
- connector services admin limitations in read-only mode **67**
- connector **39**
- Connector **71**
- Connector Setup wizard **71**
- connector URL **36**

- connector-va **57**
- connectors, installing additional **69**
- customer experience **15**

## D

- data, transfer **32**
- database **13, 28**
- database failover **66**
- deployment
  - checklists **13**
  - preparation **12**
- directory, adding **47**
- disable account **45**
- disable an account **45**
- DNS entries for KDC service **75**
- DNS, TTL Setting **67**
- DNS server redirect **67**
- DNS service location lookup **42, 44**
- domain **47**
- domain\_krb.properties file **42, 44**

## E

- external access **53**
- external database, Configurator **32**

## F

- failover **57–59, 61–63**
- failover order for resources **65**
- failover, configure database for **66**
- forward DNS **12**
- FQDN **35**

## G

- gateway-va **57**

## H

- hardware
  - ESX **9**
  - requirements **9**
- high availability **58, 62**
- HTTP proxy **25, 57**
- hznAdminTool, resource failover **65**

## I

- IdP hostname **36**
- importing OVA **64**

Integrated Windows Authentication **47**  
 integrating with Active Directory **40**  
 intended audience **5**  
 internal database **19**  
 IP Address on cloned machines **60**  
 IP Pools **19**

## J

JDBC, change on secondary data center **65**  
 join domain **47**

## K

KDC  
     create DNS entries **75**  
     initialize in Identity Manager **74**  
     setting up **73**  
 KDC realm **73**  
 KDC server certificates **73**  
 KDC subdomain **73**  
 Kerberos authentication, setting up KDC **73**  
 Kerberos realm **73**  
 Kerberos, built-in KDC **74**

## L

license **25**  
 limitations in read-only mode **67**  
 Linux  
     SUSE **5**  
     system administrator **5**  
 load balancer **53, 56**  
 log bundle **37**  
 logging **37**

## M

Microsoft SQL database **28**  
 Microsoft Windows Preview **13**  
 multi-data center, DNS redirect **67**  
 multi-domain **40**  
 multiple virtual appliance **59**  
 multiple virtual machines **57**  
 multiple data centers **63**

## N

network configuration, requirements **9**

## O

oracle database **29**  
 OVA file  
     deploy **17**  
     install **17**  
 overview, install **7**

## P

passwords, change **38**  
 PostgreSQL database **31**  
 primary data center **63**  
 proxy server settings **25, 57**

## R

read-only mode **63, 65**  
 read-only mode limitations **67**  
 read-only mode, end user functionality **67**  
 realm, KDC **73**  
 redundancy **57–59, 61, 62**  
 reverse lookup **12**  
 reverse DNS **12**  
 reverse proxy **56**  
 runtime-config.properties file **44, 65**

## S

secondary data center **63, 64**  
 self-signed certificate **33**  
 service URL **35**  
 service-va **57, 59**  
 single forest active directory **40**  
 siteaware.subnet property **44**  
 SMTP server **38**  
 SMTP Server **13**  
 SRV lookup **42, 44**  
 SSL certificate, major certificate authority **55**  
 start cloud KDC **74**  
 sticky sessions, load balancer **53**  
 SUSE Linux **5**  
 sync settings **46**  
 syslog server **36**

## T

timeout, load balancer **53**  
 troubleshooting domain\_krb.properties **45**  
 TTL Settings for DNS **67**

## U

User Attributes page **45**  
 users, user attributes **46**

## V

vCenter, credentials **13**  
 virtual appliance, requirements **9**  
 VMware Identity Manager service URL **35**

## W

Windows, system administrator **5**  
 worker **39**

Workspace  
  deploy **17**  
  install **17**  
workspace portal, OVA **70**

**X**

X-forwarded-for headers **53**

