Installing and Configuring VMware Identity Manager for Windows

FEB 2019

VMware Workspace ONE Access 3.3
VMware Identity Manager 3.3

vmware®

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

https://docs.vmware.com/

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

Contents

About Installing and Configuring VMware Identity Manager for Windows

Installing and Configuring VMware Identity Manager provides information about installing and configuring the VMware Identity Manager service on Windows servers for on premises deployments. When the installation is finished, you can use the VMware Identity Manager console to entitle users to managed multi-device access to your organization's applications, including Web applications, Horizon applications and desktops, and Citrix published resources. The guide also explains how to configure your deployment for high availability.

Intended Audience

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

VMware Identity Manager Services Overview

1

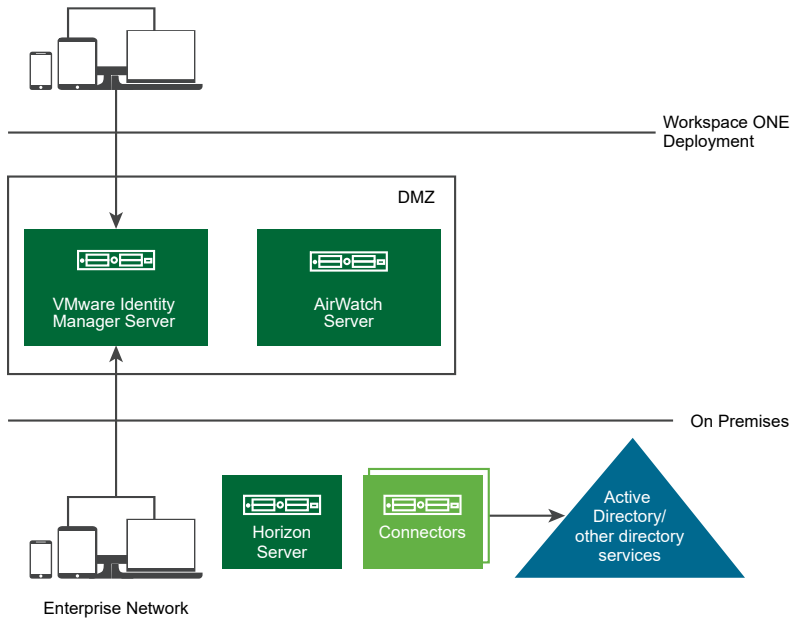
VMware Identity Manager is the identity and access management component of Workspace ONE. Alongside Workspace ONE UEM and VMware Horizon, VMware Identity Manager can deploy a universal application catalog that includes web, native, and virtual applications.

VMware Identity Manager is also crucial to deploying mobile single sign-on (SSO) and conditional access which includes device management and compliance checks. VMware Identity Manager is available both in shared SaaS and on premises deployment models.

This guide describes how to deploy VMware Identity Manager for Windows in an on premises environment, including high availability and load balancer configurations. Recommended deployment patterns and how to size your database, connector, and VMware Identity Manager servers based on the size of your organization are described in the *Preparing to Install VMware Identity Manager* chapter.

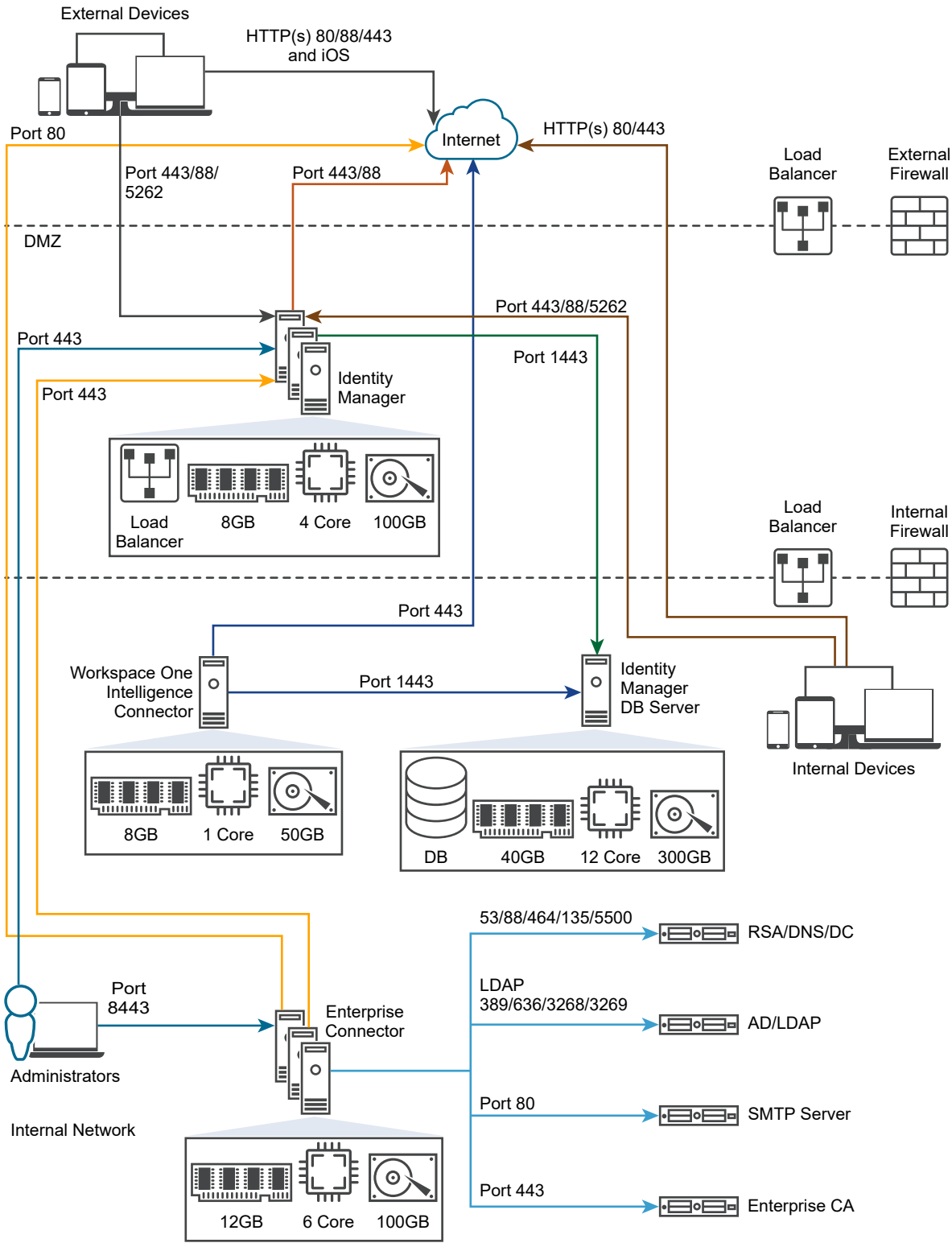
The VMware Identity Manager for Windows Deployment Model figure shows the high-level deployment pattern for Workspace ONE. The Workspace ONE UEM device service and VMware Identity Manager service are deployed in the DMZ where devices can access the services directly. The VMware Horizon service is deployed in the internal network.

Figure 1-1. VMware Identity Manager for Windows Deployment Model



The VMware Identity Manager Architecture Diagram for Typical Deployments figure shows a detailed diagram with the load balancer configuration required for clustered VMware Identity Manager.

Figure 1-2. VMWare Identity Manager Architecture Diagram for Typical Deployments



Preparing to Install VMware Identity Manager for Windows

2

The VMware Identity Manager service can be installed in a new standalone server or in a cluster of three or more nodes.

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

This chapter includes the following topics:

System and Network Configuration Requirements

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

Hardware Sizing Requirements

Ensure that you meet the hardware requirements for VMware Identity Manager installations for Windows.

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

If you install additional, standalone connectors, ensure that you meet the following requirements.

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

Software Requirements for Windows Installation

Ensure your VMware Identity Manager Windows server meets the following software requirements.

Requirement	Notes
Supported versions of Windows Server ■ Windows Server 2008 R2 ■ Windows Server 2012 R2 ■ Windows Server 2016	
PowerShell 4.0 or later	Active Directory module for PowerShell (RSAT-AD-PowerShell)
JRE 1.8 installed	The VMware Identity Manager installer installs the latest version if it is not installed before deployment. If your JRE is an older version, the installer automatically updates the version, but does not remove the existing JRE. You must manually uninstall earlier versions.
RabbitMQ Server	The VMware Identity Manager installer installs RabbitgMQ server, if it is not installed before deployment.
Erlang	The VMware Identity Manager installer installs Erlang, if it is not installed before deployment.
Notepad++	Recommend Notepad++ when making configuration edits. Notepad++ preserves the line break. Do not use Notepad.

Database Requirements

Set up VMware Identity Manager with an external Microsoft SQL database to store and organize server data.

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

The following requirements apply to an external SQL Server database. The exact specifications needed for your SQL server depend on the size and needs of your deployment.

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

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

Network Configuration Requirements

Component	Minimum Requirement
DNS record and IP address	IP address and DNS record VMware Identity Manager uses either the hostname.domainname or hostname.workgroupname during the install. These names must be set to match the DNS name of the server.
Firewall port	Ensure that the inbound firewall port 443 is open for users outside the network to the VMware Identity Manager instance or the load balancer.
Reverse Proxy	Deploy a reverse proxy such as F5 Access Policy Manager in the DMZ to allow users to securely access the VMware Identity Manager user portal remotely. VMware Unified Access Gateway 2.8 and later supports reverse proxy functionality to allow users to securely access the VMware Identity Manager unified catalog remotely. Unified Access Gateway can be deployed in the DMZ behind the load balancers front-ending the VMware Identity Manager appliance.

Port Requirements

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

- To sync users and groups from Active Directory, VMware Identity Manager must connect to Active Directory.

Port	Protocol	Source	Target	Description
443	HTTPS	Load Balancer	VMware Identity Manager machine	
443	HTTPS	VMware Identity Manager machine	Load Balancer	Needed to validate the load balancer FQDN when it is set.
443, 8443	HTTPS/ HTTP	VMware Identity Manager machine	VMware Identity Manager machine	For all VMware Identity Manager instances in a cluster, and across clusters in different data centers.

Port	Protocol	Source	Target	Description
443	HTTPS	Browsers	VMware Identity Manager machine	
443	HTTPS	VMware Identity Manager machine	discovery.awmdm.com	Access for Workspace ONE application autodiscovery
443	HTTPS	VMware Identity Manager machine	catalog.vmwareidentity.com	Access to Cloud Catalog
8443	HTTPS	Browsers	VMware Identity Manager machine	Administrator Port
25	SMTP	VMware Identity Manager machine	SMTP	Port to relay outbound mail
389 636 3268 3269	LDAP LDAPS MSFT-GC MSFT-GC-SSL	VMware Identity Manager machine	Active Directory	Default values are shown. These ports are configurable.
5500	UDP	VMware Identity Manager machine	RSA SecurID system	Default value is shown. This port is configurable.
53	TCP/UDP	VMware Identity Manager machine	DNS server	Every virtual appliance must have access to the DNS server on port 53 and allow incoming SSH traffic on port 22.
88, 464, 135, 445	TCP/UDP	VMware Identity Manager machine	Domain controller	
9300	TCP	VMware Identity Manager machine	VMware Identity Manager machine	Audit needs
54328	UDP			
5701	TCP	VMware Identity Manager machine	VMware Identity Manager machine	Hazelcast cache
40002 40003	TCP	VMware Identity Manager machine	VMware Identity Manager machine	Ehcache
1433	TCP	VMware Identity Manager machine	Database	Microsoft SQL default port is 1433
443		VMware Identity Manager machine	View server	Access to View server

Port	Protocol	Source	Target	Description
80, 443	TCP	VMware Identity Manager machine	Integration Broker server	Connection to the Integration Broker. Port option depends on whether a certificate is installed on the Integration Broker server
443	HTTPS	VMware Identity Manager macine	AirWatch REST API	For device compliance checking and for the AirWatch Cloud Connector password authentication method, if that is used.
88	UDP	Unified Access Gateway	VMware Identity Manager machine	UDP port to open for mobile SSO
5262	TCP	Android mobile device	AirWatch HTTPS proxy service	AirWatch Tunnel client routes traffic to the HTTPS proxy for Android devices.
88 443	UDP HTTPS/TCP	iOS mobile device	VMware Identity Manager machine	Port used for Kerberos traffic from iOS devices to the hosted cloud KDC service.
514	UDP	VMware Identity Manager machine	syslog server	UDP For external syslog server, if configured
88	UDP	VMware Identity Manager machine	Hybrid KDC Server in the cloud. Hostname is kdc.<realm>. For example, kdc.op.vmwareidentity.com	UDP port used to authenticate iOS Mobile SSO auth adapter configuration updates that are saved to the cloud KDC service. This port is only used if the Hybrid KDC iOS Mobile SSO feature is used.

Supported Directories

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

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

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

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

Supported Web Browsers to Access the VMware Identity Manager Console

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

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

Supported Browsers to Access the Workspace ONE Portal

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

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

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

Create DNS Records and IP Addresses

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

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

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

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

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

This example shows reverse DNS records and IP addresses.

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

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

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

Planning for Kerberos Authentication

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

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

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

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

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

Using a Unix/Linux-based DNS Server

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

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

Create the VMware Identity Manager Service Database

The VMware Identity Manager service requires an external Microsoft SQL Server database to store and organize server data. Your database administrator must prepare an empty Microsoft SQL Server database and schema before you install VMware Identity Manager.

When you connect to the Microsoft SQL server, you enter the name of the instance you want to connect to and the authentication mode. You can select either Windows Authentication mode and specify the domain\username or SQL Server Authentication mode and specify the local user name and password.

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

You can use Microsoft SQL Server to set up a high availability database environment.

Database Server Prerequisites

Before configuring the Microsoft SQL database, make sure that the hardware and software requirements are correct for your deployment.

To size your servers correctly, see System and Network Configuration Requirements .

SQL Server Software Requirements

- SQL Server 2012, SQL Server 2014, or SQL Server 2016 with Client Tools (SQL Management Studio, Reporting Services, Integration Services, SQL Server Agent, latest service packs). Ensure the SQL Servers are 64-bit (OS and SQL Server). Only Standard and Enterprise Editions are supported.
- .NET 4.6.2 is required to run the database installer. If you do not want to install .NET on to your database server, then run the database installer from another Workspace ONE UEM server or a jump server where .NET can be installed.
- Ensure the SQL Server Agent Windows service is set to Automatic or Automatic (Delayed) as the start type for the service. If set to manual, the SQL Server Agent Windows service must be manually started before database installation.

TCP/IP Enabled

Use TCP/IP to connect to the database and disable Named Pipes. In the SQL Server Configuration Manager, navigate to the SQL Server Network Configuration page and select Protocols for MSSQLSERVER.

Configure the Microsoft SQL Database with Windows Authentication Mode

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

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

Note The default collation is case-sensitive.

Prerequisites

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

Procedure

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

   The editor window appears.

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

3. To create the database with the default schema named **saas**, enter the following commands in the editor window.

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


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

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

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

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

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

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

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

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

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

Results

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

Configure Microsoft SQL Database Using Local SQL Server Authentication Mode

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

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

Note The default database collation is case-sensitive.

Prerequisites

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

Procedure

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

   The editor window appears.

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

3. To create the database with the default schema named **saas**, enter the following commands in the editor window.

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


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

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

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

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

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

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

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

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

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

Results

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

Confirm Microsoft SQL Database Is Correctly Configured

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

Prerequisites

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

Procedure

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

The editor window appears.

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

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

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


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

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

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

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

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

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

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

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

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

Change Database-Level Roles

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

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

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

Prerequisites

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

Procedure

1 In the Microsoft SQL Server management Studio session as an admin with sysadmin privileges, connect to the database instance <saasdb> for VMware Identity Manager.

2 Revoke the role **db_owner** on the database, enter the following command

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

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

Authentication Mode	Command

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

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

Change SQL Server Database Auto Growth Settings

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

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

Procedure

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

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

3 To change the auto growth setting, run the following command.

```
ALTER DATABASE <saasdb>

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

GO
```

Results

The auto growth setting is changed to 128 MB.

Deployment Checklists

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

Directory Information

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

Table 2-3. Active Directory Domain Controller Information Checklist

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

Table 2-4. LDAP Directory Server Information Checklist

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

SSL Certificates

You can add an SSL certificate after you deploy the VMware Identity Manager service.

Table 2-5. SSL Certificate Information Checklist

Information to Gather	List the Information
SSL certificate	
Private key	

License Key

Table 2-6. VMware Identity Manager License Key Information Checklist

Information to Gather	List the Information
License key	

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

External Database

Table 2-7. External Database Information Checklist

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

Customer Experience Improvement Program

3

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

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

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

Deploying the VMware Identity Manager Machine Behind a Load Balancer

4

In an enterprise environment, the recommended VMware identity Manager machine configuration is to deploy a three-node cluster of the VMware Identity Manager service for high availability. After the first IDM node is installed, configured, and tested behind the load balancer, a script is run on the first node to create a copy of the first instance. This copied file is used to create the other nodes in the cluster.

The VMware Identity Manager architecture diagram demonstrates how you can deploy the VMware Identity Manager environment.

See Chapter 1 VMware Identity Manager Services Overview.

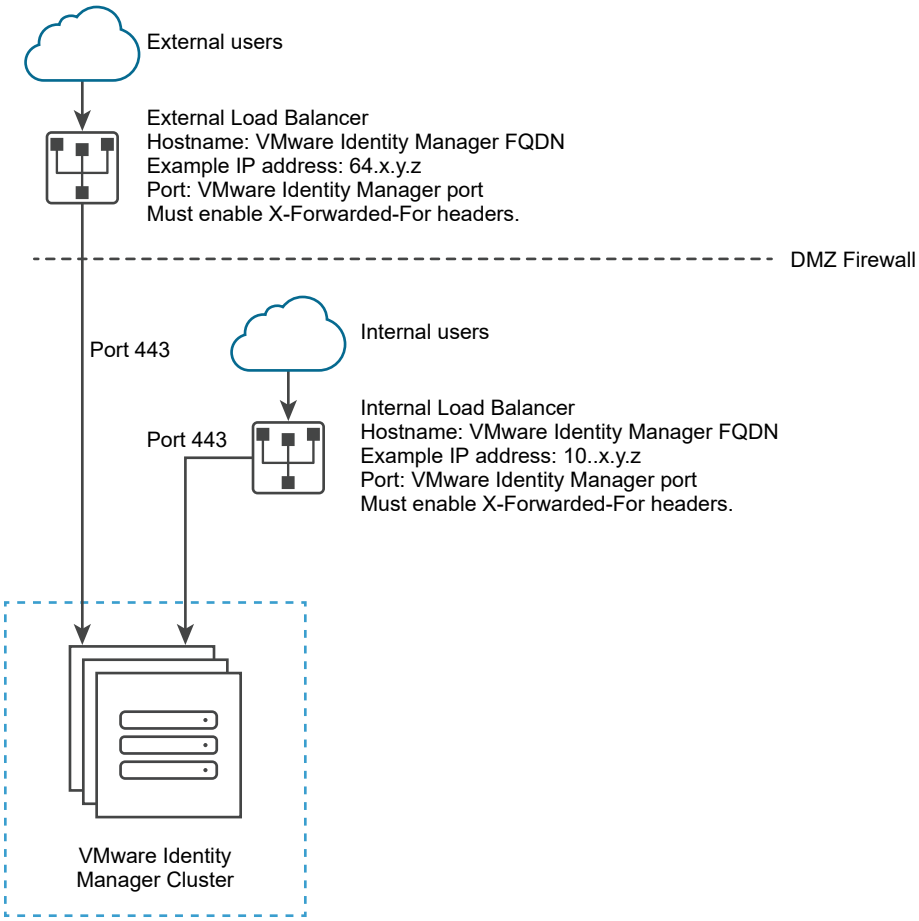
This chapter includes the following topics:

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

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

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

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



Specify VMware Identity Manager FQDN during Deployment

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

The VMware Identity Manager machine always runs on port 443. You can use a different port number for the load balancer. If you use a different port number, you must specify it during deployment. Do not use 8443 as the port number, as this port number is the VMware identity Manager administrative port and is unique for each machine in a cluster.

Load Balancer Settings to Configure

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

- X-Forwarded-For Headers

You must enable X-Forwarded-For headers on your load balancer. VMware Identity Manager identifies the source IP address in the X-Forwarded-For headers and determines which authentication method to use based on the source IP address. See the documentation provided by your load balancer vendor for more information.

- Load Balancer Timeout

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

- Enable Sticky Sessions

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

- WebSocket support

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

- Ciphers with forward secrecy

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

  ECDHE_ECDSA_AES and ECDHE_RSA_AES in GCM or CBC mode

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

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

Setting up VMware Identity Manager Service

5

This chapter includes the following topics:

Install VMware Identity Manager

Run the VMware Identity Manager installer on a Windows server that meets all the system configuration requirements listed.

Prerequisites

See System and Network Configuration Requirements .

Procedure

1 Double-click the VMware Identity Manager installer.

  Run the installer from an account with administrator privileges.

2 On the Welcome dialog box, click **Next**.

The installer verifies prerequisites on the server. If required software such as .NET or TLS is not installed, you are prompted to install the software and to restart the server. After restarting, run the VMware Identity Manager installer again.

3 Accept the End User License Agreement (EULA), then click **Next**.

4 On the **Customer Experience Improvement Program** dialog box, the default action is set to Yes.

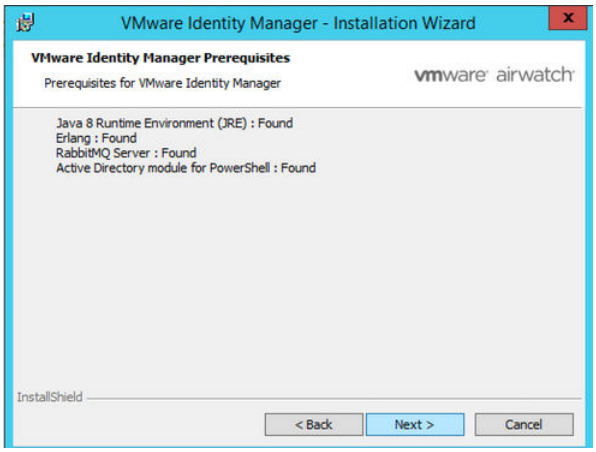
This product participates in VMware's Customer Experience Improvement Program ("CEIP"). Details regarding the data collected through CEIP and the purposes for which it is used by VMware are set forth at the Trust & Assurance Center at http://www.vmware.com/trustvmware/ceip.html. If you prefer not to participate in VMware's CEIP for this product, uncheck the box.

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

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

5 The VMware Identity Manager prerequisites are listed. The installer checks for the required modules. You are prompted to install any missing modules.

Figure 5-1. Confirming Prerequisites Installed



6 Select the directory in which to install theVMware Identity Manager service.

7 If this node is the first service instance being installed in the cluster, click **Next**.

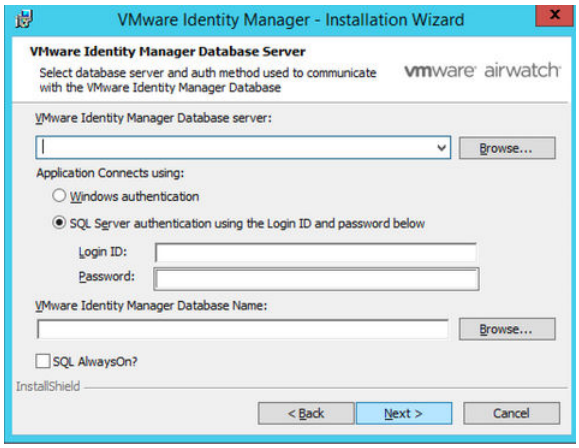
When you install additional instances in the cluster, you select the check box and browser to the exported ZIP file for the first instance to import.

8 The host name and port 443 are prepopulated in the Configuration dialog box. Click**Next**.

9 In the Database Server dialog box, select the VMware Identity Manager database server instance to connect to and the authentication mode.

Option	Description
VMware Identity Manager Database Server	Enter the database FQDN, or click **Browse** to select the database server URL from the list. Example of the database FQDN, enter **`http://MyDBServer`**.
Application Connects using	You can select either **Windows Authentication** mode or **SQL Server Authentication mode**. For SQL Server Authentication, enter the local user name and password.
VMware Identity Manager Database Name	Enter the database name you created when you set up the MySQL database or browse the SQL server to select the name from a list, if you renamed the database.
SQL AlwaysON?	Enabling **SQL AlwaysON** to set `MultiSubNetFailover` to `True` in the SQL server to enable faster failover on the SQL server. The SQL Server AlwaysOn capability is a combination of failover clustering and database mirroring/log shipping. It allows for multiple read copies of your database and a single copy for read-write operations. If your network has the bandwidth to support the traffic generated, the Identity Manager database supports AlwaysOn.

Figure 5-2. Database Configuration with SQL AlwayOn Option



Click **Next**.

The installer validates that the database is configured correctly. If the configuration is not correct, error messages are displayed and the installation cannot continue. Correct the problems described in the error messages. See Confirm Microsoft SQL Database Is Correctly Configured.

10 In the VMware Identity Manager Service Account dialog box, select the check box if you want to run the service as a Windows domain user.

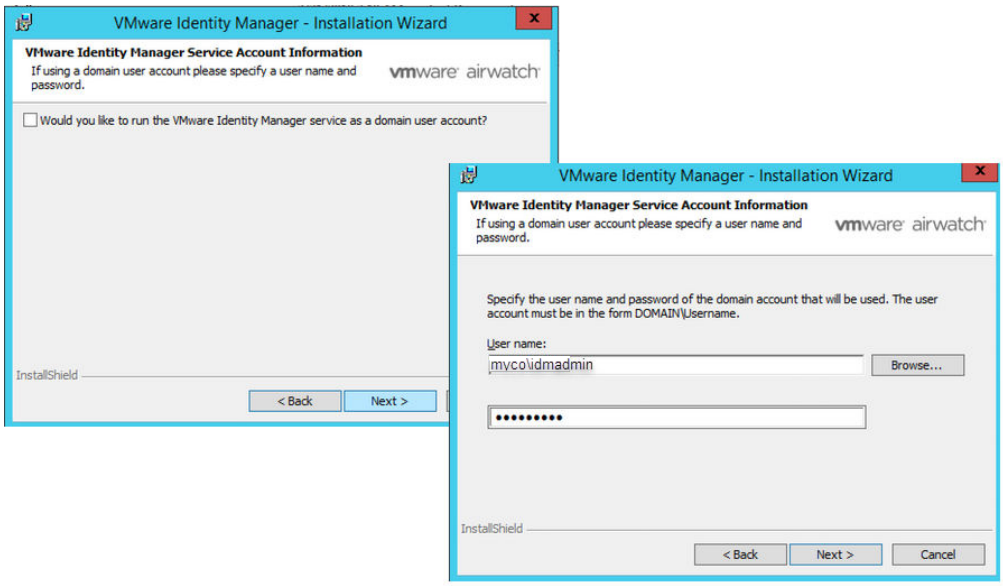
Run the service as a domain user in the following cases.

- If you plan to connect to Active Directory (Integrated Windows Authentication).
- If you plan to use Kerberos authentication.

- If you plan to integrate Horizon View with VMware Identity Manager and want to use the Perform Directory Sync or Configuring 5.x Connection Server options.

If you do not use a domain user account, the service is run as a local system.

Figure 5-3. Domain User Account Configuration

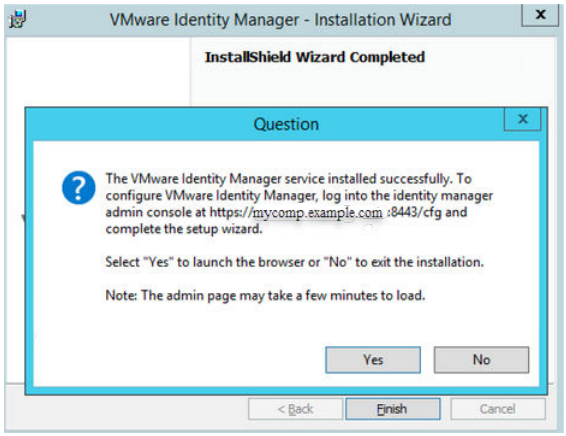


11 Click **Install** to begin the installation.

12 Click **Finish**.

The VMware Identity Server is initialized and the VMware Identity Manager URL to log in to the VMware Identity Manager console to finish the setup is displayed. To finish the setup now, click **Yes**. Otherwise, note the URL to log in later.

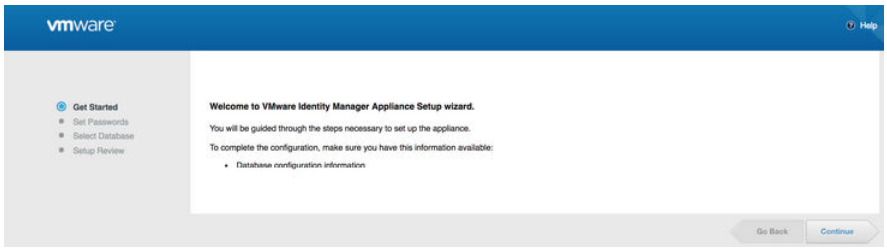
Figure 5-4. Information About Logging in to Identity Manager Console



What to do next

Run the VMware Identity Manager Setup wizard to finish the service configuration.

Figure 5-5. Setup Wizard



Using Setup Wizard to Complete the Installation

After the VMware Identity Manager is deployed, you use the Setup wizard to set the machine admin password for VMware Identity Manager, accept the self-signed certificate, and verify the database JDBC URL.

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

Procedure

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

   During the installation, a self-signed certificate is deployed. You can update to a signed-certificate after the initial set up.
3. In the Get Started page, click **Continue**.
4. In the Set Passwords page, configure the Appliance Administrator password. The admin user password must be at least 6 characters in length. Click **Continue**.

   The **admin** user account is used to manage the appliance settings.
5. In the Select Database page, the database JDBC URL is displayed.

   The connection to the database is configured and the database is initialized.

Results

The **Setup is complete** page is displayed.

What to do next

Set up Active Directory. See Set Up Active Directory or LDAP Directory Connections.

Deploying the VMware Identity Manager Machine Behind a Load Balancer

In an enterprise environment, the recommended VMware identity Manager machine configuration is to deploy a three-node cluster of the VMware Identity Manager service for high availability. After the first IDM node is installed, configured, and tested behind the load balancer, a script is run on the first node to create a copy of the first instance. This copied file is used to create the other nodes in the cluster.

The VMware Identity Manager architecture diagram demonstrates how you can deploy the VMware Identity Manager environment.

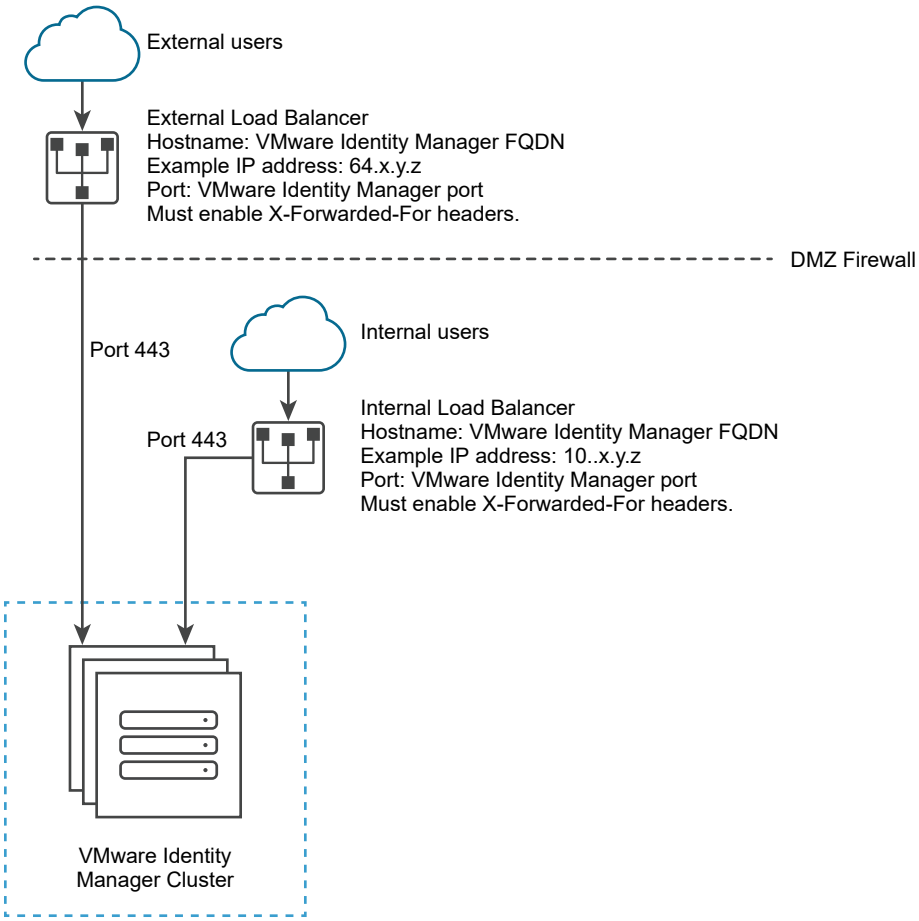
See Chapter 1 VMware Identity Manager Services Overview.

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

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

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

Figure 5-6. External Load Balancer Proxy with Virtual Machines



Specify VMware Identity Manager FQDN during Deployment

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

The VMware Identity Manager machine always runs on port 443. You can use a different port number for the load balancer. If you use a different port number, you must specify it during deployment. Do not use 8443 as the port number, as this port number is the VMware identity Manager administrative port and is unique for each machine in a cluster.

Load Balancer Settings to Configure

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

- X-Forwarded-For Headers

You must enable X-Forwarded-For headers on your load balancer. VMware Identity Manager identifies the source IP address in the X-Forwarded-For headers and determines which authentication method to use based on the source IP address. See the documentation provided by your load balancer vendor for more information.

- Load Balancer Timeout

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

- Enable Sticky Sessions

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

- WebSocket support

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

- Ciphers with forward secrecy

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

  ECDHE_ECDSA_AES and ECDHE_RSA_AES in GCM or CBC mode

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

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

Apply VMware Identity Manager Root Certificate to the Load Balancer

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

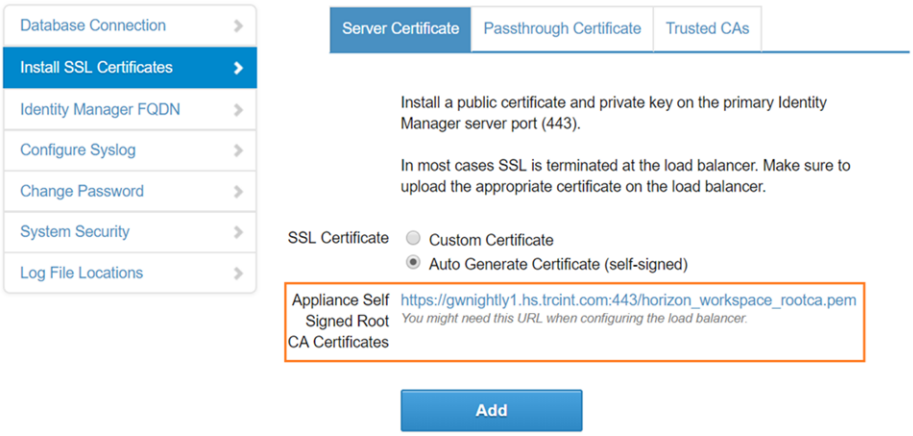
The VMware Identity Manager root certificate can be downloaded from the **Appliance Settings > Manage Configuration > Install SSL Certificates > Server Certificate** page in the VMware Identity Manager administration console.

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

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

Procedure

1. In the VMware Identity Manager console, select the **Appliance Settings** tab, then click **VA Configuration > Manage Configuration**.
2. In the dialog box that appears, enter the admin user password.
3. Select **Install SSL Certificates > Server Certificate**.
4. Click the **Appliance Self Signed Root CA Certificates** link.



   The certificate is displayed.

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

What to do next

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

Apply Load Balancer Root Certificate to VMware Identity Manager

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

Procedure

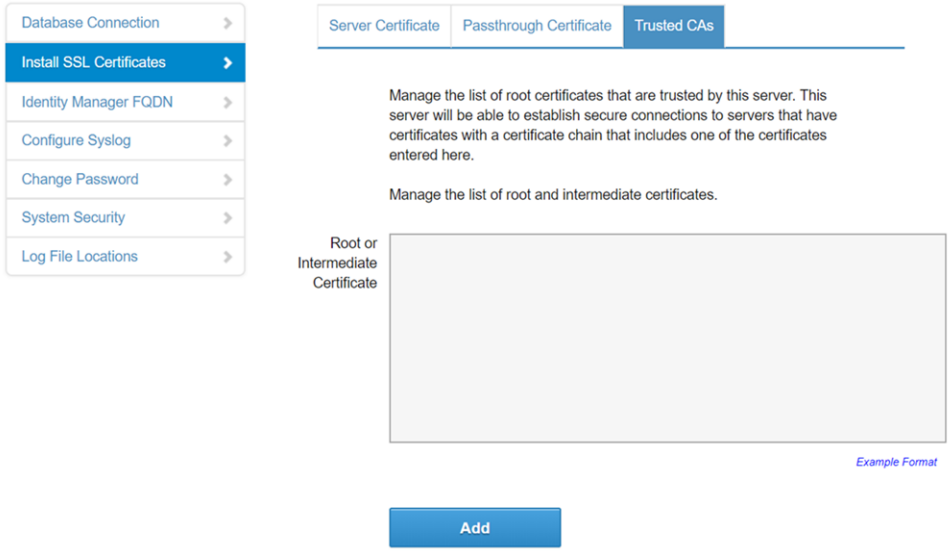
1. Obtain the load balancer root certificate.

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

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

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

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



6 Click **Add**.

Configuring Failover and Redundancy in a Single Data Center (Windows)

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

You install and configure VMware Identity Manager on a Windows server, and then you run a script to create an ENC file that is a copy of the first instance of the VMware Identity Manager for Windows with the same configuration as the original.

Before you create a copy of the first instance, you must configure the first node behind a load balancer and change its Fully Qualified Domain Name (FQDN) to match the load balancer FQDN. Also, complete the directory configuration in the VMware Identity Manager service before you create the ENC file.

You run theVMware Identity Manager for Windows installer on each node and import the copied ENC file. You can customize these nodes to change the name, network settings, and other properties, as required. Each node has a different IP address. This IP address must follow the same guidelines as the IP address for the first node. The IP address must resolve to a valid host name using forward and reverse DNS.

All nodes in the cluster are identical and nearly stateless copies of each other. Syncing to Active Directory and to resources that are configured, such as Horizon, is enabled on the first node, but disabled on all other nodes in the cluster.

Network Partitions

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

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

Change VMware Identity Manager FQDN to Load Balancer FQDN

Before you copy the instance of the VMware Identity Manager machine, you must change its Fully Qualified Domain Name (FQDN) to match the load balancer FQDN.

Prerequisites

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

Procedure

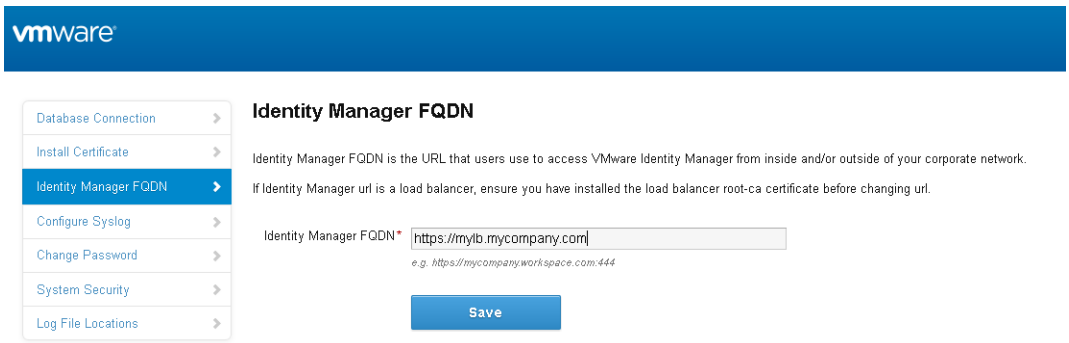
1. Log in to the VMware Identity Manager administration console.
2. Select the **Appliance Settings** tab.
3. In the Virtual Appliance Configuration page, click **Manage Configuration**.
4. Enter your administrator password to log in.
5. Click **Identity Manager Configuration**.
6. In the **Identity Manager FQDN** field, change the host name part of the URL from the VMware Identity Manager host name to the load balancer host name.

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

   `https://myservice.example.com`

   to the following:

   `https://mylb.example.com`



7 Click **Save**.

Results

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

What to do next

Run the script to generate an ENC file of the first node for VMware Identity Manager for Windows.

Adding Nodes to Create a VMware Identity Manager Cluster

To create a cluster with the VMware Identity Manager service after you install the first instance of VMware Identity Manager, you copy that instance to create an image with the same configuration as the original.

When using multiple VMware Identity Manager services, three or more nodes are required.

Note The VMware Identity Manager component includes Elasticsearch, a search and analytics engine, and Elasticsearch has a known limitation with cluster of two nodes.

Prerequisites

The first VMware Identity Manager instance deployed and tested.

A cluster config file created from the first instance configuration.

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

2 Click **Cluster File Location**.

3 Enter the password to use to encrypt and decrypt the cluster file.

4 Click **Prepare cluster bundle**. A ZIP file of the instance of the VMware Identity Manager is created.

5 Download the ZIP file to a location that you can get to.

Procedure

1 Run the VMware Identity Manager for Windows installer on each machine that is being configured in the cluster.

   Run the installer from an account with administrator privileges.

2 On the Welcome dialog box, click **Next**.

   The installer verifies prerequisites on the server. If the required software such as .NET or TLS is not installed, you are prompted to install the software and to restart the server. After restarting, run the VMware Identity Manager installer again.

3 Accept the End User License Agreement (EULA), then click **Next**.

4 The **Customer Experience Improvement Program** radio button is selected by default. Deselect the radio button if you do not want the data collected.

   VMware collects anonymous data about your deployment to improve VMware's response to user requirements.

5 The VMware Identity Manager prerequisites are listed. The installer checks for the required modules. You are prompted to install any missing modules.

6 Select the directory in which to install theVMware Identity Manager service.

7 On the Configuration dialog box, select the **Are you joining an existing cluster** check box and browse to the cluster config (ENC) file of the first instance.

   By default the file is located at `< INSTALL_DIR>\VMwareIdentityManager\usr\local\horizon \< filename>.enc`.

8 Enter the cluster password created for the cluster config ENC file and click **Next**.

9 Click **Install** to begin the installation.

10 To finish the installation, click **Finish**.

   All the VMware Identity Manager configuration files are copied to the server.

What to do next

Add the cloned machine to the load balancer.

Removing a Node from a Cluster

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

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

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

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

Disassociate Connector Component from Domains, Directory Sync Settings, and Built-in Identity Provider

Before you can remove a node from a VMware Identity Manager cluster, you must ensure that the node's connector component is not joined to any domains, is not being used as a sync connector, and is not associated with the Built-in identity provider.

Prerequisites

You must log in as a tenant administrator, that is, a local administrator on the VMware Identity Manager service. A domain administrator synced from the enterprise directory does not have the necessary permissions.

Procedure

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

   The Connectors page is displayed.
3. If the connector component of the node is being used as the sync connector for any directory, change the directory's Sync Connector setting to use another connector instead.
   a. In the **Associated Directory** column in the Connectors page, view the directories with which the connector component is associated.
   b. Click a directory link.
   c. In the **Directory Sync and Authentication** section of the directory page, check the value of the **Sync Connector** option.
   d. If the connector component is being used as the sync connector, select another connector for the **Sync Connector** option and click **Save**.
   e. Repeat these steps for all the directories with which the connector component is associated.

4 If the connector component is associated with the Built-in identity provider, remove it from the identity provider.

   a In the Connectors page, in the **Identity Provider** column, view the identity providers with which the connector component is associated.

   b If the Built-in identity provider is listed, click on the link.

   c In the identity provider page, in the **Connectors** section, click the delete icon next to the connector.

What to do next

Remove the node from the cluster.

Remove the Node from the Cluster

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

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

Prerequisites

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

Procedure

1 Shut down the node virtual machine.

   a Log in to the vCenter Server instance.

   b Right-click the node virtual machine and select **Power > Power Off**.

2 Remove the node from the load balancer.

3 In the VMware Identity Manager console, remove the node.

   a Log in to the VMware Identity Manager console as a local administrator.

   b Click the down arrow on the **Dashboard** tab and select **System Diagnostics Dashboard**.

   c Locate the node you want to remove.

   The node displays the following status:

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

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

Results

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

What to do next

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

Set Up Active Directory or LDAP Directory Connections

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

The following types of directories are supported.

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

Prerequisites

- Review *Directory Integration with VMware Identity Manager* for requirements and limitations.
- Your Active Directory or LDAP directory information.
- When multi-forest Active Directory is configured and the Domain Local group contains members from domains in different forests, the Bind DN user used on the VMware Identity Manager directory page must be added to the Administrators group of the domain in which Domain Local group resides. If this is not done, these members are missing from the Domain Local group.

  Note The VMware Identity Manager service must be configured to run as the Windows domain user to use multi-forest Active Directory.

- The list of the user attributes you want to use as filters, and a list of the groups you want to add to VMware Identity Manager.

Procedure

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

   You are logged in as a Local Admin. The Directories page appears. Before you add a directory, ensure that you review *Directory Integration with VMware Identity Manager* for requirements and limitations.

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

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

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

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

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

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

4 Click **Save**.

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

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

You can also create a local directory in the service. For more information about using local directories, see the VMware Identity Manager Administration guide.

7 For Active Directory, follow these steps.

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

b Provide the connection information.

Option	Description
Active Directory over LDAP	1 In the **Sync Connector** text box, select the connector you want to use to sync users and groups from Active Directory to the VMware Identity Manager directory. A connector component is always available with the VMware Identity Manager service by default. This connector appears in the drop-down menu. If you install multiple VMware Identity Manager appliances for high availability, the connector component of each appears in the list. 2 In the **Authentication** text box, select **Yes** if you want to use this Active Directory to authenticate users. If you want to use a third-party identity provider to authenticate users, click **No**. After you configure the Active Directory connection to sync users and groups, go to the **Identity & Access Management > Manage > Identity Providers** page to add the third-party identity provider for authentication. 3 In the **Directory Search Attribute** text box, select the account attribute that contains username. 4 If the Active Directory uses DNS Service Location lookup, make the following selections. ■ In the **Server Location** section, select the **This Directory supports DNS Service Location** check box. ■ If the Active Directory requires STARTTLS encryption, select the **This Directory requires all connections to use SSL** check box in the **Certificates** section and copy and paste the Active Directory Root CA certificate into the **SSL Certificate** text box. Ensure the certificate is in PEM format and include the "BEGIN CERTIFICATE" and "END CERTIFICATE" lines. **Note** If the Active Directory requires STARTTLS and you do not provide the certificate, you cannot create the directory. 5 If the Active Directory does not use DNS Service Location lookup, make the following selections. ■ In the **Server Location** section, verify that the **This Directory supports DNS Service Location** check box is not selected and enter the Active Directory server host name and port number. To configure the directory as a global catalog, see the Multi-Domain, Single Forest Active Directory Environment section in "Active Directory Environments" in *Directory Integration with VMware Identity Manager*. ■ If the Active Directory requires access over SSL, select the **This Directory requires all connections to use SSL** check box in the **Certificates** section and copy and paste the Active Directory Root CA certificate into the **SSL Certificate** text box.

Option	Description
	Ensure the certificate is in PEM format and include the "BEGIN CERTIFICATE" and "END CERTIFICATE" lines. **Note** If the Active Directory requires SSL and you do not provide the certificate, you cannot create the directory. 6 In the **Allow Change Password** section, select **Enable Change Password** if you want to allow users to reset their passwords from the VMware Identity Manager login page if the password expires or if the Active Directory administrator resets the user's password. 7 In the **Base DN** text box, enter the DN from which to start account searches. For example, OU=myUnit,DC=myCorp,DC=com. 8 In the **Bind DN** text box, enter the account that can search for users. For example, CN=binduser,OU=myUnit,DC=myCorp,DC=com. **Note** Using a Bind DN user account with a non-expiring password is recommended. 9 After you enter the Bind password, click **Test Connection** to verify that the directory can connect to your Active Directory.
Active Directory (Integrated Windows Authentication)	1 In the **Sync Connector** text box, select the connector you want to use to sync users and groups from Active Directory to the VMware Identity Manager directory. A connector component is always available with the VMware Identity Manager service by default. This connector appears in the drop-down list. If you install multiple VMware Identity Manager appliances for high availability, the connector component of each appears in the list. 2 In the **Authentication** text box, if you want to use this Active Directory to authenticate users, click **Yes**. If you want to use a third-party identity provider to authenticate users, click **No**. After you configure the Active Directory connection to sync users and groups, go to the **Identity & Access Management > Manage > Identity Providers** page to add the third-party identity provider for authentication. 3 In the **Directory Search Attribute** text box, select the account attribute that contains username. 4 If the Active Directory requires STARTTLS encryption, select the **This Directory requires all connections to use STARTTLS** check box in the **Certificates** section and copy and paste the Active Directory Root CA certificate into the **SSL Certificate** text box. Ensure the certificate is in PEM format and include the "BEGIN CERTIFICATE" and "END CERTIFICATE" lines. If the directory has multiple domains, add the Root CA certificates for all domains, one at a time. **Note** If the Active Directory requires STARTTLS and you do not provide the certificate, you cannot create the directory. 5 In the **Allow Change Password** section, select **Enable Change Password** if you want to allow users to reset their passwords from the VMware Identity Manager login page if the password expires or if the Active Directory administrator resets the user's password.

Option	Description
	6 In the **Bind User UPN** field, enter the User Principal Name of the user who can authenticate with the domain. For example, username@example.com. **Note** Using a Bind DN user account with a non-expiring password is recommended. 7 Enter the Bind DN User password.

c Click **Save & Next**.

The page with the list of domains appears.

8 For LDAP directories, follow these steps.

a Provide the connection information.

Option	Description
Directory Name	A name for the directory you are creating in VMware Identity Manager.
Directory Sync and Authentication	1 In the **Sync Connector** text box, select the connector you want to use to sync users and groups from your LDAP directory to the VMware Identity Manager directory. A connector component is always available with the VMware Identity Manager service by default. This connector appears in the drop-down list. If you install multiple VMware Identity Manager appliances for high availability, the connector component of each appears in the list. You do not need a separate connector for an LDAP directory. A connector can support multiple directories, regardless of whether they are Active Directory or LDAP directories. 2 In the **Authentication** text box, select **Yes** if you want to use this LDAP directory to authenticate users. If you want to use a third-party identity provider to authenticate users, select **No**. After you add the directory connection to sync users and groups, go to the **Identity & Access Management > Manage > Identity Providers page** to add the third-party identity provider for authentication. 3 In the **Directory Search Attribute** text box, specify the LDAP directory attribute to be used for user name. If the attribute is not listed, select **Custom** and enter the attribute name. For example, **cn**.
Server Location	Enter the LDAP Directory server host and port number. For the server host, you can specify either the fully-qualified domain name or the IP address. For example, **myLDAPserver.example.com** or **100.00.00.0**. If you have a cluster of servers behind a load balancer, enter the load balancer information instead.
LDAP Configuration	Specify the LDAP search filters and attributes that VMware Identity Manager can use to query your LDAP directory. Default values are provided based on the core LDAP schema. **LDAP Queries** ■ **Get groups**: The search filter for obtaining group objects. For example: **(objectClass=group)** ■ **Get bind user**: The search filter for obtaining the bind user object, that is, the user that can bind to the directory. For example: **(objectClass=person)** ■ **Get user**: The search filter for obtaining users to sync. For example:**(&(objectClass=user)(objectCategory=person))** **Attributes** ■ **Membership**: The attribute that is used in your LDAP directory to define the members of a group. For example: **member**

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

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

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

c Click **Save & Next**.

The page listing the domain appears.

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

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

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

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

Click **Next**.

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

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

11 Click **Next**.

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

Option	Description
Specify the group DNs	To select groups, you specify one or more group DNs and select the groups under them. a Click **+** and specify the group DN. For example, CN=users,DC=example,DC=company,DC=com. **Important** Specify group DNs that are under the Base DN that you entered. If a group DN is outside the Base DN, users from that DN is synced but is not able to log in. b Click **Find Groups**. The **Groups to Sync** column lists the number of groups found in the DN. c To select all the groups in the DN, click **Select All**, otherwise click **Select** and select the specific groups to sync. **Note** If you have multiple groups with the same name in your LDAP directory, you must specify unique names for them in VMware Identity Manager. You can change the name while selecting the group. **Note** When you sync a group, any users that do not have Domain Users as their primary group in Active Directory are not synced.
Sync nested group members	The **Sync nested group members** option is enabled by default. When this option is enabled, all the users that belong directly to the group you select as well as all the users that belong to nested groups under it are synced. Note that the nested groups are not synced; only the users that belong to the nested groups are synced. In the VMware Identity Manager directory, these users will be members of the parent group that you selected for sync. If the **Sync nested group members** option is disabled, when you specify a group to sync, all the users that belong directly to that group are synced. Users that belong to nested groups under it are not synced. Disabling this option is useful for large Active Directory configurations where traversing a group tree is resource and time intensive. If you disable this option, ensure that you select all the groups whose users you want to sync.

13 Click **Next**.

14 Specify additional users to sync, if required.

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

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

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

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

15 Click **Next**.

16 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.

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

Results

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

What to do next

For information about setting up a load balancer or a high-availability configuration, see Chapter 4 Deploying the VMware Identity Manager Machine Behind a Load Balancer.

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*.

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

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

Procedure

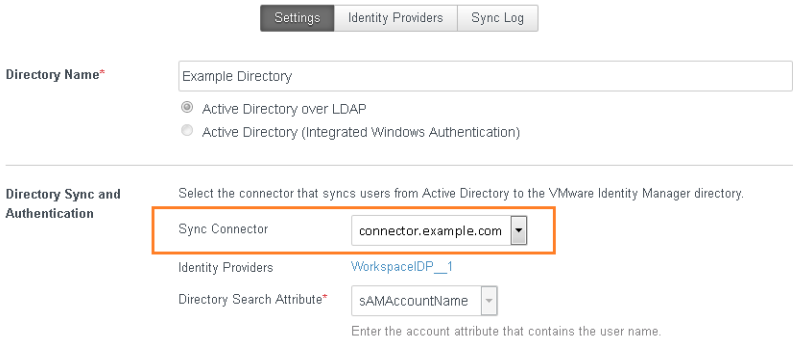
1 Log in to the VMware Identity Manager console.

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

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

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

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



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

6 Click **Save**.

Adding Whitelist IP Addresses to Your External Firewall

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

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

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

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

Enabling Proxy Settings After Installation

The VMware Identity Manager machine 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 machine.

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

Procedure

1. Log in to the VMware Identity Manager console and navigate to the Appliance Settings > VA Configuration page.
2. Click **Manage Configuration** and then click **Proxy Configuration**.
3. **Enable** Proxy.
4. In **Proxy host with port** text box, enter the proxy name and port. For example, `proxyhost.example.com:3128`
5. In the **Non-Proxied hosts** text box, enter the non-proxy hosts that are accessed without going through the proxy server.

   Use a comma to separate a list of host names.
6. Click **Save**.

Enter the License Key

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

Procedure

1 Log in to the VMware Identity Manager console.

2 Select the **Appliance Settings** tab, then click **License**.

3 In the License Settings page, enter the license key and click **Save**.

Managing VMware Identity Manager Configuration Settings

6

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

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

Page Name	Setting Description
Database Connection	The database connection setting, either Internal or External, is enabled. You can change the database type. When you select External Database, you enter the external database URL, user name, and password. To set up an external database, see Create the VMware Identity Manager Service Database.
Install SSL Certificates	On the tabs on this page, you can install an SSL certificate for VMware Identity Manager, download the self-signed VMware Identity Manager root certificate, and install trusted root certificates. For example, if VMware Identity Manager is configured behind a load balancer, you can install the load balancer's root certificate. **Note** The **Passthrough Certificate** tab is used only when certificate authentication is configured on the embedded connector in a DMZ deployment scenario. See *Deploying VMware Identity Manager in the DMZ* for information. See Using SSL Certificates.
Identity Manager FQDN	On this page, you can view or change the VMware Identity Manager FQDN. The VMware Identity Manager FQDN is the URL that users use to access the service.
Change Password	On this page, you can change the VMware Identity Manager admin user password.
Proxy Configuration (VMware Identity Manager for Windows)	Configure HTTPS proxy settings

Page Name	Setting Description
Log File Locations	You can download the logs in a zip file. See Log File Information.
Cluster File Location VMware Identity Manager for Windows)	You can create an encrypted file of the VMware Identity Manager configuration instance. This ENC file can be downloaded and used to create a cluster of VMware Identity Manager nodes.

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

This chapter includes the following topics:

- Change Appliance Configuration Settings
- Using SSL Certificates
- Configure VMware Identity Manager to Use an External Database
- Modifying the VMware Identity Manager Service URL
- Modifying the Connector URL
- Log File Information
- Manage Your Password
- Configure SMTP Settings

Change Appliance Configuration Settings

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

Procedure

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

What to do next

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

Using SSL Certificates

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

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

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

If you deploy VMware Identity Manager with the self-signed SSL certificate, the root CA certificate must be available as a trusted CA for any client who accesses the VMware Identity Manager service. The clients can include end user machines, load balancers, proxies, and so on. You can download the root CA from the **Install SSL Certificates > Server Certificates** page.

Installing an SSL Certificate for the VMware Identity Manager Service

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

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

Prerequisites

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

Procedure

1. In the VMware Identity Manager console, click the **Appliance Settings** tab.
2. Click **Manage Configuration** and enter the admin user password.
3. Select **Install SSL Certificates > Server Certificate**.
4. In the SSL Certificate field, select **Custom Certificate**.

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

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

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

7 Click **Add.**

Example: Certificate Examples

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

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

Installing Trusted Root Certificates

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

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

Procedure

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

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

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

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

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

5 Click **Add.**

Installing a Passthrough Certificate

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

Configure VMware Identity Manager to Use an External Database

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

Prerequisites

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

Procedure

1 In the VMware Identity Manager console, click **Appliance Settings** and select **VA Configuration**.

2 Click **Manage Configuration**.

3 Log in with the VMware Identity Manager administrator password.

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

5 Enter information about the database connection.

a Enter the JDBC URL of the Microsoft SQL database server.

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

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

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

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

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

What to do next

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

Modifying the VMware Identity Manager Service URL

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

Procedure

1 Log into the VMware Identity Manager console.

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

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

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

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

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

5 Click **Save**.

What to do next

Enable the new portal user interface.

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

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

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

Modifying the Connector URL

You can change the connector URL by updating the identity provider hostname in the VMware Identity Manager console.

Procedure

1 Log in to the VMware Identity Manager console.

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

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

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

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

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

5 Click **Save**.

Log File Information

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

Table 6-1. Log Files

Component	Location of Log File Linux	Location of Log File Windows	Description
Identity Manager Service Logs	`/opt/vmware/horizon/workspace/logs/horizon.log`	`<INSTALL_DIR>\opt\vmware\horizon\workspace\logs\horizon.log`	Information about activity on the service, such as entitlements, users, and groups.
Configurator Logs	`/opt/vmware/horizon/workspace/logs/configurator.log`	`<INSTALL_DIR>\opt\vmware\horizon\workspace\logs\configurator.log`	Requests that the Configurator receives from the REST client and the web interface.

Table 6-1. Log Files (continued)

Component	Location of Log File Linux	Location of Log File Windows	Description
Connector Logs	`/opt/vmware/horizon/workspace/logs/connector.log`	`<INSTALL_DIR>\opt\vmware\horizon\workspace\logs\connector.log`	A record of each request received from the Web interface. Each log entry also includes the request URL, timestamp, and exceptions. No sync actions are recorded.
	`/opt/vmware/horizon/workspace/logs/connector-dir-sync.log`	*`InstallDirectory`*`\IDMConnector\opt\vmware\horizon\workspace\logs\connector-dir-sync.log`	Messages related to directory sync.
Apache Tomcat Logs	`/opt/vmware/horizon/workspace/logs/catalina.log`	`<INSTALL_DIR>\opt\vmware\horizon\workspace\logs\catalina.log`	Apache Tomcat records of messages that are not recorded in other log files.

Collect Log Information

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

Collect the logs from each appliance in your environment.

Procedure

1. Log in to the VMware Identity Manager console.
2. Select the **Appliance Settings** tab and click **Manage Configuration**.
3. Click **Log File Locations** and click **Prepare log bundle**.

   The information is collected into a tar.gz file that can be downloaded.
4. Download the prepared bundle.

What to do next

To collect all logs, do this on each appliance.

Setting the VMware Identity Manager Service Log Level to DEBUG

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

Procedure

1. Log in to the machine.

2 Change to the path to the `conf` directory.

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

   For Windows, go to `\usr\local\horizon\conf\`.

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

   a Edit the file.

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

      For example, change:

      `rootLogger.level=INFO`

      to:

      `rootLogger.level=DEBUG`

   c Save the file.

      A restart of the service or system is not required.

Manage Your Password

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

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

Note If you are unable to log in and need to reset the password, you can use the hznSetAdminPassword.bat script to reset the password. See Resetting Admin User Password for VMware Identity Manager for Windows.

Procedure

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

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

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

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

4 Enter the new password.

5 Click **Save**.

Resetting Admin User Password for VMware Identity Manager for Windows

You can change the VMware Identity Manager service admin user password from the connector admin pages at https://<hostnameFQDN>:8443/cfg/login. However, if you are unable to log in and need to reset the password, you can use the hznSetAdminPassword.bat script to reset the password.

Procedure

1. In the Windows server, open the Command Prompt window.
2. Navigate to the IDM_INSTALL_DIR>\usr\local\horizon\bin folder.

   ```
   cd <IDM_INSTALL_DIR>\usr\local\horizon\bin
   ```

   where IDM_INSTALL_DIR is the VMware Identity Manager service installation directory.
3. Run the following command.

   ```
   hznAdminTool.bat setSystemAdminPassword –pass newPassword
   ```

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

Configure SMTP Settings

Configure SMTP server settings to receive email notifications from the VMware Identity Manager service. For example, notification emails are sent when new local users are created, when a password is reset, or with the auto discovery verification token.

Procedure

1. Log in to the VMware Identity Manager console.
2. Click the **Appliance Settings** tab and click **SMTP**.
3. Enter the SMTP server host name.

   For example: `smtp.example.com`
4. Enter the SMTP server port number.

   For example: `25`
5. (Optional) If the SMTP server requires authentication, enter the user name and password.
6. Click **Save**.

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

   a Log in to the VMware Identity Manager machine.

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

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

   For example:

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

   c Save the file.

   d Restart the machine.

   ```
   <install dir>\usr\local\horizon\scripts\horizonService.bat restart
   ```

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

Upgrading Java on the VMware Identity Manager Server

7

VMware Identity Manager requires the Java Runtime Environment (JRE).

The required JRE version is packaged with the VMware Identity Manager installer. When you upgrade VMware Identity Manager, you are prompted to upgrade the JRE version too.

If you want to upgrade JRE on the VMware Identity Manager server at any other time, follow these steps to ensure that the VMware Identity Manager service continues to work correctly after the JRE upgrade.

Note If JRE gets upgraded automatically, follow steps 3-4 after the upgrade.

Procedure

1. Stop the VMware IDM, Elasticsearch, and VMware IDM Cert Proxy services.
2. Install the new JRE version.
3. Update the `JAVA_HOME` environment variable to point to the new JRE.
4. Restart the VMware IDM, Elasticsearch, and VMware IDM Cert Proxy services.

Monitoring VMware Identity Manager

8

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

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

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

This chapter includes the following topics:

Hardware Load Capacity Monitoring Recommendations

Use these monitoring standards to ensure server health.

Metrics to Capture

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

Alerts and Thresholds

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

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

Strategies for Capture

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

VMware Identity Manager URL Endpoints for Monitoring

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

Health Checks for Load Balancers

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

Component	Health Check	Expected Return	Notes
	Certificate adapter: `:7443/SAAS/API/1.0/REST/system/health/heartbeat`	String: ok Http: 200	Frequency every 30 seconds
VMware Identity Manager Connector	`/hc/API/1.0/REST/system/health/allOk`	String: true Http: 200	Frequency every 30 seconds
Integration Broker	`/IB/API/RestServiceImpl.svc/ibhealthcheck`	String: All Ok Http: 200	Frequency every 30 seconds
	XenApp 7.x Integration: `/IB/API/RestServiceImpl.svc/hznxenapp/admin/xenfarminfo?computerName=&xenappversion=Version7x`	String: 'SiteName' Http: 200	Frequency every 5 minutes
	XenApp 6.x Integration: `/IB/API/RestServiceImpl.svc/hznxenapp/admin/xenfarminfo?computerName=&xenappversion=Version65orLater`	String: 'FarmName' Http: 200	Frequency every 5 minutes

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

Additional Health Checks for Monitoring

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

VMware Identity Manager Service Monitoring and Health

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

or

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

Raw output:

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

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


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

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

URL call: /catalog-portal/services/health

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

Raw output:


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


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

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

VMware Identity Manager Connector Monitoring and Health

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

Raw output:


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

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

VMware Identity Manager Integration Broker Monitoring and Health

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

Raw output:

```
“All Ok”
```

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

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

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

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

Raw output:

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

Raw output exception:

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

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

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

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

Raw output:

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

Displaying Additional Information in Health Check API

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

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

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

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

```
AnalyticsUrl: "http://198.51.100.0"
ElasticsearchServiceOk: "true"
EhCacheClusterPeers: ""
ElasticsearchMasterNode: "198.51.100.1"
ElasticsearchIndicesCount: "13"
ElasticsearchDocsCount: "11173"
AuditPollInterval: "1000"
```

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

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

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

Procedure

1 Log in to the VMware Identity Manager server.

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

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

3 Save the file.

4 Restart the service.

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

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

System Logging

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

VMware Identity Manager Service and Connector Logging

Log Locations

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

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

Log	Purpose
greenbox_web.log	Log which contains all user interface interactions for web and mobile
horizon.log	VMware Identity Manager service log which includes Identity Adapters, RabbitMQ, Elasticsearch, Ehcache, and other subsystems
connector.log	VMware Identity Manager connector log for all authentication methods and integrations with Horizon and Citrix
cert-proxy.log	VMware Identity Manager service CertProxy component for Android Mobile SSO
configurator.log	Requests that the Configurator receives from the REST client and the Web interface
catalina.log	Apache Tomcat records of messages that are not recorded in other log files

Integration Broker Logging

Integration Broker logs are located in the following location:

`C:\ProgramData\VMware\HorizonIntegrationBroker`

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

Change Default Memory Allocated to VMware Identity Manager Service

For precise control over the amount of memory allocated for the VMware Identity Manager service, you can change the memory allocated in Tomcat through the Windows system properties environment variables page.

When the VMware Identity Manager service is installed, the default is to set the memory setting to be half of the available memory. Usually the default setting does not need to be changed.

Procedure

1. On the VMware Identity Manager Windows machine, open the Control Panel and navigate to **Systems Properties > Advanced** tab.
2. Click **Environment Variables** at the bottom of the dialog box.
3. In the Environment Variables > User Variables section, click **New**.
4. In the **New User Variable** dialog box, enter the variable as `IDM_TOMCAT_MEM= <#>g`

   #g is the memory to allocate. 2G is the minimum memory setting to allocate, but there is no maximum.
5. Restart the service. Type the batch file command, **`horizonService.bat restart`**.

Setting Rate Limits

9

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

This chapter includes the following topics:

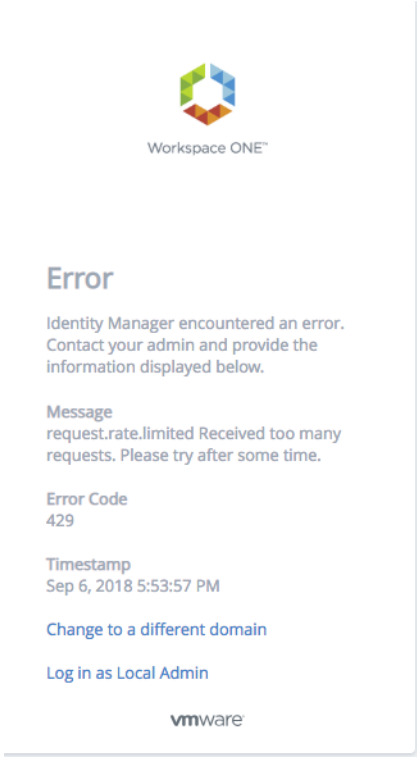
Setting Rate Limits on the VMware Identity Manager Service

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

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

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

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



No rate limits are set by default.

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

Setting Rate Limits

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

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

Method: PUT

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

Headers:

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

Path Parameters:

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

Request Body:

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

Request Body Parameters

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

Viewing Rate Limits

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

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

Method: GET

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

Headers:

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

Path Parameters:

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

Sample Output:

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

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

Setting Rate Limits on the VMware Identity Manager Connector

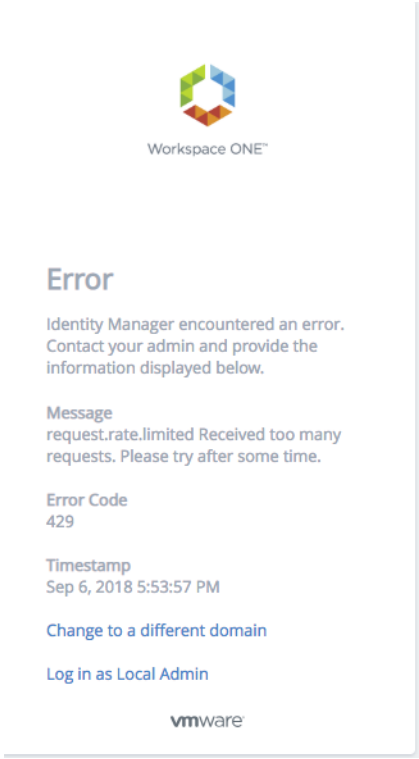
Just as you can set rate limits on the VMware Identity Manager service, you can set rate limits on the VMware Identity Manager connector.

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

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

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

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



No rate limits are set by default.

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

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

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

```
service horizon-workspace restart
```

To restart the Windows connector, run the following script:

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

Setting Rate Limits

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

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

Method: PUT

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

Headers:

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

Path Parameters:

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

Request Body:

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

Request Body Parameters

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

Viewing Rate Limits

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

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

Method: GET

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

Headers:

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

Path Parameters:

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

Sample Output:

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

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

Troubleshooting Installation and Configuration

10

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

This chapter includes the following topics:

Group Does Not Display Any Members after Directory Sync

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

Problem

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

Cause

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

Solution

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

   For example, enter **https://community.spiceworks.com/how_to/5765-configure-windows-server-to-query-an-external-ntp-server**.

2. Restart the service on all the nodes.

   ```
   <install dir>\usr\local\horizon\scripts\horizonService.bat restart
   ```

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

Users Unable to Launch Applications in Load-balanced Environment

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

Problem

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

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

Solution

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

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

Method: `GET`

Path: `/clientipresolutioninfo`

Authorization: `HZN` *`cookie_value`*

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

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

Sample JSON response:

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

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

1 Log in to the VMware Identity Manager server.

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

`service.ipsToIgnoreInXffHeader` *IPsToIgnore*

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

3 Restart the VMware IDM service.