Upgrading to VMware Identity Manager 2.8

VMware Identity Manager 2.8

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

EN-002299-00

vmware®

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

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

The VMware Web site also provides the latest product updates.

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

docfeedback@vmware.com

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

Contents

Upgrading to VMware Identity Manager 2.8 5

1 About Upgrading to VMware Identity Manager 2.8 7
- Upgrading a Cluster 8
- Preparing RabbitMQ Server Before Upgrade 8

2 Upgrading VMware Identity Manager Online 11
- Prerequisites for Online Upgrade 11
- Check for the Availability of a VMware Identity Manager Upgrade Online 12
- Configure Proxy Server Settings for the VMware Identity Manager Appliance 12
- Perform an Online Upgrade 12

3 Upgrading VMware Identity Manager Offline 15
- Prerequisites for Offline Upgrade 15
- Prepare a Local Web Server for Offline Upgrade 15
- Configure the Appliance and Perform Offline Upgrade 16

4 Configure Settings after Upgrade 19

5 Troubleshooting Upgrade Errors 21
- Checking the Upgrade Error Logs 21
- Rolling Back to Snapshots of VMware Identity Manager 21
- Collecting a Log File Bundle 22

6 Troubleshooting RabbitMQ Issues 23

Index 25

Upgrading to VMware Identity Manager 2.8

Upgrading to VMware Identity Manager 2.8 describes how to upgrade to VMware Identity Manager 2.8 from version 2.6.

If you would prefer to do a fresh installation of version 2.8, see *VMware Identity Manager Installation and Configuration*. Remember that a new installation does not preserve your existing configurations.

For information about using your upgraded VMware Identity Manager instance, see the *VMware Identity Manager Administrator's Guide*.

Intended Audience

This information is intended for anyone who installs, upgrades, and configures VMware Identity Manager. The information is written for experienced Windows or Linux system administrators who are familiar with virtual machine technology.

VMware Technical Publications Glossary

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

About Upgrading to VMware Identity Manager 2.8

1

The following upgrade paths and scenarios are supported.

Supported Upgrade Paths

The following upgrade paths are supported:

- Version 2.6 or later to 2.8

Internet Connectivity

You can upgrade VMware Identity Manager online or offline.

By default, the VMware Identity Manager appliance uses the VMware Web site for the upgrade procedure, which requires the appliance to have Internet connectivity. You must also configure proxy server settings for the appliance, if applicable.

If your virtual appliance does not have Internet connectivity, you can perform the upgrade offline. For an offline upgrade, you download the upgrade package from My VMware and set up a local Web server to host the upgrade file.

Upgrade Scenarios

- If you have deployed a single VMware Identity Manager appliance, upgrade it online or offline as described in Chapter 2, "Upgrading VMware Identity Manager Online," on page 11 or Chapter 3, "Upgrading VMware Identity Manager Offline," on page 15.

  Note Expect some downtime because all services are stopped during the upgrade. Plan the timing of your upgrade accordingly.

- If you have deployed multiple VMware Identity Manager virtual appliances in a cluster for failover or high availability, see "Upgrading a Cluster," on page 8.
- To upgrade VMware Identity Manager with no downtime in a multi-data center deployment scenario, see "Upgrading VMware Identity Manager with No Downtime" in *Installing and Configuring VMware Identity Manager*.

This chapter includes the following topics:

- "Upgrading a Cluster," on page 8
- "Preparing RabbitMQ Server Before Upgrade," on page 8

Upgrading a Cluster

If you have deployed multiple VMware Identity Manager virtual appliances in a cluster for failover or high availability, you can upgrade the nodes one at a time. Expect some downtime during upgrade and plan the timing of your upgrade accordingly.

See also "Preparing RabbitMQ Server Before Upgrade," on page 8.

Procedure

1 Take snapshots of the database and the VMware Identity Manager nodes.

2 Remove all nodes except one from the load balancer.

3 Upgrade the node that is still connected to the load balancer.

Follow the process for an online or offline upgrade, as described in Chapter 2, "Upgrading VMware Identity Manager Online," on page 11 or Chapter 3, "Upgrading VMware Identity Manager Offline," on page 15.

Important Expect some downtime during the upgrade process.

4 After the node is upgraded, leave it connected to the load balancer.

This ensures that the VMware Identity Manager service is available while you upgrade the other nodes.

5 Upgrade the other nodes one at a time.

6 After all the nodes are upgraded, add them back to the load balancer.

Preparing RabbitMQ Server Before Upgrade

If you deployed multiple VMware Identity Manager virtual appliances in a cluster, you must stop the RabbitMQ cluster on all nodes before you upgrade the VMware Identity Manager appliance.

The RabbitMQ nodes must be stopped in the reverse order that they were started. This preserves the order of the master node. To determine the start order, view the `/db/rabbitmq/data/*/nodes_running_at_shutdown` files on each server. Shut down the RabbitMQ node that lists all the nodes first. For example, if you have three nodes that were started as node1, then node2, then node3, the nodes_running_at_shutdown file on node 3 lists node1,node2,node3. Node 2 lists node1,node2. Node 1 list node1. You shut down node 3, then node 2, then node 1.

Procedure

1 Stop RabbitMQ nodes on each VMware Identity Manager appliance in the cluster. Type `rabbitmqctl stop`.

Do this for each RabbiMQ node in the cluster before continuing.

2 Verify that RabbitMQ is detached from the cluster. Type `rabbitmqctl cluster_status`.

3 Upgrade the first node. See the upgrade procedures either in Chapter 2, "Upgrading VMware Identity Manager Online," on page 11 or Chapter 3, "Upgrading VMware Identity Manager Offline," on page 15.

The VMware Identity Manager appliance is started.

4 Follow steps 2 through 4 for each node.

   As each node is upgraded, run the `rabbitmgctl cluster_status` command on the upgraded node to verify that all the nodes upgraded so far are listed in the `running_nodes` section of the output. After upgrading node 1, the `running_nodes` section lists only node1. After upgrading node 2, run the `rabbitmqctl cluster_status` command on both nodes and the `running_nodes` section should each list node1 and node2. This indicates that the RabbitMQ nodes are clustered together correctly.

When all nodes are upgraded, RabbitMQ forms a cluster with the nodes in the correct order.

Upgrading VMware Identity Manager Online 2

You can upgrade the VMware Identity Manager virtual appliance online. The virtual appliance must be able to connect to the Internet for an online upgrade.

This chapter includes the following topics:

- "Prerequisites for Online Upgrade," on page 11
- "Check for the Availability of a VMware Identity Manager Upgrade Online," on page 12
- "Configure Proxy Server Settings for the VMware Identity Manager Appliance," on page 12
- "Perform an Online Upgrade," on page 12

Prerequisites for Online Upgrade

Before you upgrade the VMware Identity Manager virtual appliance online, perform these prerequisite tasks.

- Verify that at least 2.5 GB of disk space is available on the primary root partition of the virtual appliance.
- Take a snapshot of your virtual appliance to back it up. For information about how to take snapshots, see the vSphere documentation.
- If you are using an external database, take a snapshot or backup of the database.
- Verify that VMware Identity Manager is properly configured.
- Verify that the virtual appliance can resolve and reach vapp-updates.vmware.com on port 80 over HTTP.
- If an HTTP proxy server is required for outbound HTTP access, configure the proxy server settings for the virtual appliance. See "Configure Proxy Server Settings for the VMware Identity Manager Appliance," on page 12.
- Confirm that a VMware Identity Manager upgrade exists. Run the appropriate command to check for upgrades. See "Check for the Availability of a VMware Identity Manager Upgrade Online," on page 12.

Check for the Availability of a VMware Identity Manager Upgrade Online

If your VMware Identity Manager virtual appliance can connect to the Internet, you can check for the availability of upgrades online from the appliance.

Procedure

1 Log in to the virtual appliance as the root user.

2 Run the following command to check for an online upgrade.

```
/usr/local/horizon/update/updatemgr.hzn check
```

Configure Proxy Server Settings for the VMware Identity Manager Appliance

The VMware Identity Manager virtual appliance accesses the VMware update servers through the Internet. If your network configuration provides Internet access using an HTTP proxy, you must adjust the proxy settings for the appliance.

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

Note Proxy servers that require authentication are not supported.

Prerequisites

- Verify that you have the root password for the virtual appliance.
- Verify that you have the proxy server information. Note that proxy servers that require authentication are not supported.

Procedure

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

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

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

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

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

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

```
service horizon-workspace restart
```

The VMware update servers are now available to the VMware Identity Manager virtual appliance.

Perform an Online Upgrade

If your VMware Identity Manager virtual appliance has Internet connectivity, you can upgrade the appliance online.

Prerequisites

- Ensure that you meet the prerequisites listed in "Prerequisites for Online Upgrade," on page 11.
- Verify that the virtual appliance is powered on and functioning.

Procedure

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

2 Run the following `updatemgr.hzn` command.

```
/usr/local/horizon/update/updatemgr.hzn updateinstaller
```

3 Run the following command to check that on online upgrade exists.

```
/usr/local/horizon/update/updatemgr.hzn check
```

4 Run the following command to update the appliance.

```
/usr/local/horizon/update/updatemgr.hzn update
```

Messages that occur during the upgrade are saved to the `update.log` file at `/opt/vmware/var/log/update.log`.

5 Run the `updatemgr.hzn check` command again to verify that a newer update does not exist.

```
/usr/local/horizon/update/updatemgr.hzn check
```

6 Check the version of the upgraded appliance.

```
vamicli version ––appliance
```

The new version is displayed.

7 Restart the virtual appliance.

```
reboot
```

The upgrade is complete.

Note that search and autocomplete features in the administration console will not be available for 15-20 minutes after the virtual appliance starts. In version 2.7, search indexes have been moved to Elasticsearch, a search and analytics engine embedded in the VMware Identity Manager appliance. The migration process can take up to 15-20 minutes after the virtual appliance starts.

Also note that for search and autocomplete to work, auditing must not be disabled. You can verify the auditing setting in the **Catalog > Setting > Auditing** page.

Upgrading VMware Identity Manager Offline

3

If your VMware Identity Manager virtual appliance cannot connect to the Internet for upgrade, you can perform an offline upgrade. You must set up an upgrade repository on a local Web server and configure the appliance to use the local Web server for upgrade.

This chapter includes the following topics:

- "Prerequisites for Offline Upgrade," on page 15
- "Prepare a Local Web Server for Offline Upgrade," on page 15
- "Configure the Appliance and Perform Offline Upgrade," on page 16

Prerequisites for Offline Upgrade

Before you upgrade the VMware Identity Manager virtual appliance offline, perform these prerequisite tasks.

- Verify that at least 2.5 GB of disk space is available on the primary root partition of the virtual appliance.
- Take a snapshot of your virtual appliance to back it up. For information about how to take snapshots, see the vSphere documentation.
- If you are using an external database, take a snapshot or backup of the database.
- Verify that VMware Identity Manager is properly configured.
- Confirm that a VMware Identity Manager upgrade exists. Check the My VMware site at my.vmware.com for upgrades.
- Prepare a local Web server to host the upgrade file. See "Prepare a Local Web Server for Offline Upgrade," on page 15.

Prepare a Local Web Server for Offline Upgrade

Before you start the offline upgrade, set up the local Web server by creating a directory structure that includes a subdirectory for the VMware Identity Manager virtual appliance.

Prerequisites

- Obtain the `identity-manager-2.8.x.x-buildNumber-updaterepo.zip` file. Go to my.vmware.com and navigate to the VMware Identity Manager product download page to download the file.
- If you use an IIS Web server, configure the Web server to allow special characters in file names. You configure this in the **Request Filtering** section by selecting the **Allow double escaping** option.

Procedure

1 Create a directory on the Web server at http://*YourWebServer*/*VM*/ and copy the downloaded zip file to it.

2 Verify that your Web server includes mime types for `.sig` (text/plain) and `.sha256` (text/plain).

Without these mime types your Web server fails to check for updates.

3 Unzip the file.

The contents of the extracted ZIP file are served by http://*YourWebServer*/*VM*/.

The extracted contents of the file contain the following subdirectories: `/manifest` and `/package-pool`.

4 Run the following `updatelocal.hzn` command to check that the URL has valid update contents.

```
/usr/local/horizon/update/updatelocal.hzn checkurl http://YourWebServer/VM
```

Configure the Appliance and Perform Offline Upgrade

Configure the VMware Identity Manager appliance to point to the local Web server to perform an offline upgrade. Then upgrade the appliance.

Prerequisites

"Prepare a Local Web Server for Offline Upgrade," on page 15.

Procedure

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

2 Run the following command to configure an upgrade repository that uses a local Web server.

```
/usr/local/horizon/update/updatelocal.hzn seturl http://YourWebServer/VM/
```

Note To undo the configuration and restore the ability to perform an online upgrade, you can run the following command.

```
/usr/local/horizon/update/updatelocal.hzn setdefault
```

---

3 Perform the upgrade.

a Run the following `updatemgr.hzn` command.

```
/usr/local/horizon/update/updatemgr.hzn updateinstaller
```

b Run the following command.

```
/usr/local/horizon/update/updatemgr.hzn update
```

Messages that occur during the upgrade are saved to the `update.log` file at `/opt/vmware/var/log/update.log`.

c Run the `updatemgr.hzn check` command again to verify that a newer update does not exist.

```
/usr/local/horizon/update/updatemgr.hzn check
```

d Check the version of the upgraded appliance.

```
vamicli version --appliance
```

The command should display the new version.

e Restart the virtual appliance.

For example, from the command line run the following command.

```
reboot
```

The upgrade is complete.

Note that search and autocomplete features in the administration console will not be available for 15-20 minutes after the virtual appliance starts. In version 2.7, search indexes have been moved to Elasticsearch, a search and analytics engine embedded in the VMware Identity Manager appliance. The migration process can take up to 15-20 minutes after the virtual appliance starts.

Also note that for search and autocomplete to work, auditing must not be disabled. You can verify the auditing setting in the **Catalog > Setting > Auditing** page.

Configure Settings after Upgrade 4

After you upgrade to VMware Identity Manager 2.8, configure these settings.

- If you have set up a VMware Identity Manager cluster for failover, updating it to three nodes is recommended. This is because of a limitation of Elasticsearch, a search and analytics engine embedded in the VMware Identity Manager appliance. You may continue to use two nodes but you should be aware of a few limitations related to Elasticsearch. See "Configuring Failure and Redundancy" in *Installing and Configuring VMware Identity Manager* for more information.
- Enable the new portal user interface.
  a In the administration console, click the arrow on the **Catalog** tab and select **Settings**.
  b Select **New End User Portal UI** in the left pane and click **Enable New Portal UI**.
- Transport Layer Security (TLS) protocol 1.0 is disabled by default in VMware Identity Manager 2.8. TLS 1.1 and 1.2 are supported.

  External product issues are known to occur when TLS 1.0 is disabled. Updating your other product configurations to use TLS 1.1 or 1.2 is recommended. However, if your version of products such as Horizon, Horizon Air, Citrix, or load balancers have a dependence on TLS 1.0, you can enable TLS 1.0 in VMware Identity Manager by following the instructions in Knowledge Base article 2144805.

Troubleshooting Upgrade Errors 5

You can troubleshoot upgrade problems by reviewing the error logs. If VMware Identity Manager does not start, you can revert to a previous instance by rolling back to a snapshot.

This chapter includes the following topics:

- "Checking the Upgrade Error Logs," on page 21
- "Rolling Back to Snapshots of VMware Identity Manager," on page 21
- "Collecting a Log File Bundle," on page 22

Checking the Upgrade Error Logs

Resolve errors that occur during upgrade by reviewing the error logs. Upgrade log files are in the `/opt/vmware/var/log` directory.

Problem

After the upgrade finishes, VMware Identity Manager does not start and errors appear in the error logs.

Cause

Errors occurred during upgrade.

Solution

1 Log in to the VMware Identity Manager virtual appliance.

2 Go to the directory located at `/opt/vmware/var/log`.

3 Open the `update.log` file and review the error messages.

4 Resolve the errors and rerun the upgrade command. The upgrade command resumes from the point where it stopped.

Note Alternatively, you can revert to a snapshot and run the upgrade again.

Rolling Back to Snapshots of VMware Identity Manager

If VMware Identity Manager does not start properly after an upgrade, you can roll back to a previous instance.

Problem

After you upgrade VMware Identity Manager, it does not start correctly. You reviewed the upgrade error logs and ran the upgrade command again but it did not resolve the issue.

Cause

Errors occurred during the upgrade process.

Solution

- Revert to one of the snapshots you took as a backup of your original VMware Identity Manager instance and external database, if applicable. For information, see the vSphere documentation.

Collecting a Log File Bundle

You can collect a bundle of log files. You obtain the bundle from the VMware Identity Manager appliance configuration page.

The following log files are collected in the bundle.

Table 5-1. Log Files

Component	Location of Log File	Description
Apache Tomcat Logs (catalina.log)	`/opt/vmware/horizon/workspace/logs/catalina.log`	Apache Tomcat records messages that are not recorded in other log files.
Configurator Logs (configurator.log)	`/opt/vmware/horizon/workspace/logs/configurator.log`	Requests that the Configurator receives from the REST client and the Web interface.
Connector Logs (connector.log)	`/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.
Service Logs (horizon.log)	`/opt/vmware/horizon/workspace/logs/horizon.log`	The service log records activity that takes place on the VMware Identity Manager appliance, such as activity related to entitlements, users, and groups.
Unified Catalog Logs (greenbox_web.log)	`/opt/vmware/horizon/workspace/logs/greenbox_web.log`	Records activity related to the unified catalog.

Procedure

1 Log in to the VMware Identity Manager appliance configuration page at https://*identitymanagerURL*:8443/cfg/logs.

2 Click **Prepare log bundle**.

3 Download the bundle.

Troubleshooting RabbitMQ Issues 6

RabbitMQ service stops working after you upgrade.

Problem

RabbitMQ is not responding correctly in the upgraded cluster environment.

Solution

The RabbitMQ nodes must be stopped in the reverse order that they were started. This preserves the order of the master node. To determine the start order, view the `/db/rabbitmq/data/*/nodes_running_at_shutdown` files on each server. Shut down the node that lists all the nodes first. For example, if you have three nodes that were started, node1, then node2, then node3, the `nodes_running_at_shutdown` file on node 3 lists node1,node2,node3. Node 2 lists node1,node2. Node 1 list node1. You shut down 3, then 2, then 1.

Procedure

1 Stop RabbitMQ nodes on each VMware Identity Manager appliance in the cluster.

   Type `rabbitmqctl stop`.

   Do this for each RabbiMQ node in the cluster before going on.

2 Start the RabbitMQ node on the last node stopped.

   Type `rabbitmq-server -detached`.

3 Verify that the node started.

   Type `rabbitmqctl status`.

4 Follow steps 2 and 3 to start the other RabbitMQ nodes in the cluster in the correct order.

5 Verify that RabbitMQ is detached from the cluster.

   Type `rabbitmqctl cluster_status`.

6 Restart the VMware Identity Manager service.

   Type `service horizon-workspace restart`.

Index

C
check for upgrade online **12**
cluster, upgrade **8**
collect log bundle **22**
configure settings **19**

E
error logs **21**
errors **21**

G
glossary **5**

H
HTTP proxy **12**

I
intended audience **5**

L
local Web server **16**
log bundle **22**

N
new portal user interface **19**

O
offline upgrade **15**
online upgrade **11, 12**

P
point to local Web server **16**
prepare local Web server **15**
prerequisites for offline upgrade **15**
prerequisites for online upgrade **11**
proxy server **12**

R
rabbitMQ **8**
RabbitMQ,troubleshooting **23**
roll back to snapshot **21**

S
snapshots **21**

T
troubleshooting **21**

U
upgrade **7**
upgrade errors **21**