Upgrading VMware Identity Manager Connector

VMware Identity Manager 2.8
VMware Identity Manager 2.9.1

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-001881-05

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 VMware Identity Manager Connector

Upgrading VMware Identity Manager Connector describes how to upgrade your VMware Identity Manager Connector instance. If you would prefer to do a fresh installation, see *VMware Identity Manager Connector Installation and Configuration*. Remember that a new installation does not preserve your existing configurations.

The following upgrade paths are supported:

- From version 2.3 , 2.4, 2015.10.1, or later to the latest version available

For information about using your updated connector 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 Connector. The information is written for experienced Windows or Linux system administrators who are familiar with virtual machine technology.

About Upgrading VMware Identity Manager Connector

1

You can upgrade VMware Identity Manager Connector online or offline.

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

If your connector instance does not have an Internet connection, you can perform the upgrade offline. For an offline upgrade, you download the upgrade package and set up a local Web server to host the upgrade file.

The following upgrade paths are supported:

- From version 2.3 , 2.4, 2015.10.1, or later to the latest version available

Preparing to Upgrade VMware Identity Manager Connector 2

To prepare for the connector upgrade, you must perform a number of prerequisite tasks, such as checking for available upgrades and configuring the proxy server settings for the appliance, if applicable.

This chapter includes the following topics:

Prerequisites for Upgrade

Before you upgrade the connector, perform these prerequisite tasks.

Prerequisites for Online Upgrade

- Verify that the connector appliance can resolve and reach vapp-updates.vmware.com on port 80 over HTTP.
- Confirm that a connector upgrade exists. Run the appropriate command to check for upgrades. See "Check for the Availability of a VMware Identity Manager Connector Upgrade Online," on page 10.
- Verify that at least 2 GB of disk space is available on the primary root partition of the appliance.
- Verify that the connector is properly configured.
- Take a snapshot of your connector appliance to back it up. For information about how to take snapshots, see the vSphere documentation.
- If an HTTP proxy server is required for outbound HTTP access, configure the proxy server settings for the connector appliance. See "Configure Proxy Server Settings for the VMware Identity Manager Connector Appliance," on page 10.

Prerequisites for Offline Upgrade

- Confirm that a connector upgrade exists. Check the My VMware Downloads site at my.vmware.com for upgrades.
- Verify that at least 2 GB of disk space is available on the primary root partition of the appliance.
- Verify that the connector is properly configured.
- Take a snapshot of your connector appliance to back it up. For information about how to take snapshots, see the vSphere documentation.

- Configure the connector appliance to use a local Web server to host the upgrade file. See Chapter 4, "Performing an Offline Upgrade of VMware Identity Manager Connector," on page 13.

Check for the Availability of a VMware Identity Manager Connector Upgrade Online

If your connector appliance has Internet connectivity, you can check for the availability of upgrades online from the appliance.

Procedure

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

2 Run the following command.

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

3 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 Connector Appliance

The connector 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 connector appliance.
- Verify that you have the proxy server information.

Procedure

1 Log in to the connector 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 connector virtual appliance to use the new proxy settings.

```
service horizon-workspace restart
```

The VMware update servers are now available to the connector appliance.

Performing an Online Upgrade of VMware Identity Manager Connector

3

You can upgrade your VMware Identity Manager Connector instance online.

Prerequisites

- You have met the prerequisites listed in Chapter 2, "Preparing to Upgrade VMware Identity Manager Connector," on page 9.
- Verify that the connector appliance is powered on and functioning.

Procedure

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

2 Run the following 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 connector appliance.

```
reboot
```

8 Repeat the preceding steps for each connector appliance in your VMware Identity Manager deployment.

The connector upgrade is complete.

Performing an Offline Upgrade of VMware Identity Manager Connector

4

If your VMware Identity Manager Connector 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 connector appliance to use the local Web server for upgrade.

This chapter includes the following topics:

Prepare a Local Web Server for Offline Upgrade

Before you start the offline connector upgrade, prepare the local Web server by creating a directory structure that includes a subdirectory for the connector appliance.

Prerequisites

- Download the `identity-manager-connector-`*`versionNumber-buildNumber`*`-updaterepo.zip` file from My VMware. Go to my.vmware.com, navigate to the VMware Identity Manager Download page, and download the file listed under **VMware Identity Manager Connector offline upgrade package**.
- 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 Connector and Perform Offline Upgrade

Configure the connector 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 13.

Procedure

1 Log in to the connector 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 command.

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

   b Run the following command to check the version of the available upgrade.

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

   c Run the following command to update the connector.

   ```
   /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`.

   d Run the `updatemgr.hzn check` command again.

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

   e Check the version of the upgraded appliance.

   ```
   vamicli version --appliance
   ```

   The command should display the new version.

   f Restart the connector appliance.

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

   ```
   reboot
   ```

4 Repeat the preceding steps for each connector appliance in your VMware Identity Manager deployment.

The connector upgrade is complete.

Configure Settings after Upgrading Connector

5

After you upgrade to connector 2016.3.1.0 or later, configure these settings.

- If you use ThinApps, Kerberos authentication, or Active Directory (Integrated Windows Authentication) directories, you must leave the domain and then rejoin it. This is required for all the connector virtual appliances in your deployment.
  a Click the **Identity & Access Management** tab.
  b Click **Setup**.
  c In the Connectors page, for each connector that is being used for ThinApps integration, Kerberos authentication, or an Active Directory (Integrated Windows Authentication) directory, click **Leave Domain**.
  d Click **Join Domain** to join the domain again.

    To join the domain, you need Active Directory credentials with the privileges to join the domain. See "Integrating with Active Directory" in *Installing and Configuring VMware Identity Manager* for more information about joining a domain.
  e If you are using Kerberos authentication, enable the Kerberos authentication adapter again. To access the Auth Adapters page, in the Connectors page click the appropriate link in the **Worker** column and select the **Auth Adapters** tab.
  f Verify that the other authentication adapters you are using are enabled.
- If you are using Active Directory (Integrated Windows Authentication), or Active Directory over LDAP with the **This Directory supports DNS Service Location** option enabled, save the directory's Domains page.
  a Click the **Identity & Access Management** tab.
  b In the Directories page, click the directory.
  c Provide the password for the Bind DN user and click **Save**.
  d Click **Sync Settings** on the left of the page and select the **Domains** tab.

e Click **Save**.

Note In connector 2016.3.1.0 and later, a `domain_krb.properties` file is automatically created and auto-populated with domain controllers when a directory with DNS Service Location enabled is created. When you save the Domains page after upgrade, if you had a `domain_krb.properties` file in your original deployment, the file is updated with domains that you may have added subsequently and that were not in the file. If you did not have a `domain_krb.properties` file in your original deployment, the file is created and auto-populated with domain controllers. See "Integrating with Active Directory" in *Installing and Configuring VMware Identity Manager* for more information about the `domain_krb.properties` file.

Troubleshooting Upgrade Errors 6

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

This chapter includes the following topics:

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, the connector does not start and errors appear in the error logs.

Cause

Errors occurred during upgrade.

Solution

1 Log in to the connector appliance.

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

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 update again.

Rolling Back to Snapshots of Connector

If the connector does not start properly after an upgrade, you can roll back to a previous instance.

Problem

After you upgrade your connector instance, 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 connector instance. For information, see the vSphere documentation.

Collecting a Log File Bundle

You can collect a bundle of log files to send to VMware support. You obtain the bundle from the connector configuration page.

The following log files are collected in the bundle.

Table 6-1. 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.

Procedure

1 Log in to the connector configuration page at https://*connectorURL*:8443/cfg/logs.

2 Click **Prepare log bundle**.

3 Download the bundle and send it to VMware support.

Index