Upgrade to VMware Identity Manager 3.3 (Windows)

SEP 2018

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/

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

About Upgrading to the Latest VMware Identity Manager for Windows Version

Upgrading to the Latest VMware Identity Manager (Windows) describes how to upgrade the Windows-based VMware Identity Manager machine to 3.3 from 3.2.0.1.

For information about upgrading VMware Identity Manager for Linux, see *Upgrading to VMware Identity Manager 3.3 (Linux)*.

Intended Audience

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

Prepare for Your Upgrade 1

The upgrade process does not differ significantly from the installation process. The values and settings you configured are automatically populated. You can verify the settings and select Next through the installer.

Supported Upgrade Path

To upgrade to version 3.3, VMware Identity Manager must be at version 3.2.0.1.

VMware Identity Manager 3.1 for Windows was installed as part of the AirWatch installation for AirWatch versions 9.2. through .3.x. To upgrade from 3.1 to 3.3, see the Migrate VMware Identity Manager for Windows to 3.3 guide.

Prerequisite Steps

Before you begin the upgrade, make sure that the following steps are complete.

- Take a snapshot of the database and the VMware Identity Manager nodes before upgrading to the latest version.
- If you revoked the db_owner role on the Microsoft SQL database, you must add the role back before performing the upgrade, otherwise the upgrade fails. See Add the db_owner Role Before Upgrade.
- To upgrade a VMware Identity Manager server equipped with SQL server availability groups, you must disable availability groups before you upgrade the server. After the upgrade, you must re-enable availability groups. See Disable SQL Server AlwayOn Availability Groups Before Upgrading

This chapter includes the following topics:

Add the db_owner Role Before Upgrade

If you revoked the db_owner role on the Microsoft SQL database, you must add it back before performing an upgrade to the latest version of VMware Identity Manager.

Prerequisites

Review the Installing and Configuring VMware Identity Manager (Windows), prerequisites information about creating the database.

Add the db_owner role to the same user that was used during installation:

Procedure

1. Log in to the Microsoft SQL Server Management Studio as a user with sysadmin privileges.
2. Connect to the database instance for VMware Identity Manager.
3. Enter the following commands.

   If you are using Windows Authentication mode, use the following commands:

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

   Make sure that you replace <*saasdb*> with your database name and <*domain\username*> with the relevant domain and user name.

   If you are using SQL Server Authentication mode, use the following commands:

   ```
   USE <saasdb>;
   ALTER ROLE db_owner ADD MEMBER <loginusername>; GO
   ```

   Make sure that you replace <*saasdb*> with your database name and <*loginusername*> with the relevant user name.

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`

Disable SQL Server AlwayOn Availability Groups Before Upgrading

If you enable Microsoft SQL AlwaysON, before you upgrade a VMware Identity Manager server, you must disable availability groups.

Procedure

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

2 To disable availability groups, enter the following command.

```
USE master;
ALTER AVAILABILITY GROUP <groupname> REMOVE DATABASE <saasdb>;
```

Re-Enable AlwaysOn Availability Groups

After you upgrade a VMware Identity Manager server, you must re-enable AlwayON availability groups.

Procedure

1. In the Microsoft SQL Server management Studio sessions as an admin with sysadmin privileges, connect to the database instance for VMware Identity Manager (<saasdb>).
2. To re-enable availability groups, enter the following command.

```
USE master;
ALTER AVAILABILITY GROUP <groupname> ADD DATABASE <saasdb>;
```

3. To resync all the secondary nodes, run the following command.

```
ALTER DATABASE <saasdb> SET HADR AVAILABILITY GROUP = <groupname>;
```

Upgrading Server in the Cluster (Windows) 2

For each node in the cluster, you upgrade VMware Identity Manager for Windows. Expect some downtime during the upgrade and plan the timing of your upgrade accordingly.

Prerequisites

- Stop all nodes except one from the load balancer.

Procedure

1. Double-click the VMware Identity Manager installer.

   Run the installer from an account with administrator privileges.
2. To start the upgrade, click **Next**.
3. Accept the End User License Agreement (EULA), then click **Next**.
4. If the Customer Experience Improvement Program is not enabled, you are asked to participate in the program. 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, deselect 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.
6. Select the directory in which to install theVMware Identity Manager service.
7. In the configuration dialog box, confirm the Internal Server Hostname and port number 443 are correct and click **Next**.

8 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 and enter the user name and password of the domain account to use. The user name must be in the form DOMAIN\Username.

   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 with the company's KDC.
   - If you plan to integrate Horizon (View) with VMware Identity Manager and want to use the Perform Directory Sync.

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

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

   During the upgrade, the following actions are performed.

   - The files in that directory are upgraded to latest version of VMware Identity Manager.

10 Click **Finish**.

What to do next

Upgrade the other nodes in the cluster.

If you disabled SQL Server availability groups, re-enable the availability groups. See Re-Enable AlwaysOn Availability Groups

If you added the db_owner role for the upgrade, you can disable this role. See Change Database-Level Roles

Windows_Post-Upgrade Configuration

3

After you upgrade to VMware Identity Manager 3.3, you might need to configure some of the settings.

Enable Cert Proxy for Android Mobile Single Sign-On for Diagnostic Monitoring

If Android Mobile Single Sign-on is configured, after upgrading VMware Identity Manger, you must enable Cert Proxy through the UI to activate diagnostic monitoring.

Go to the **Appliance Settings > Mobile SSO Android SSO cert proxy config** page and select **Enable Cert Proxy**. Click **Save**.

Log4j Configuration Files

If any `log4j` configuration files in a VMware Identity Manager instance were edited, new versions of the files are not automatically installed during the upgrade. However, after the upgrade, the logs controlled by those files will not work.

To resolve this issue:

1 Log in to the Windows machine.

2 Search for `log4j` files with the `.rpmnew` suffix.

```
find / –name "**log4j.properties.rpmnew"
```

3 For each file found, copy the new file to the corresponding old `log4j` file without the `.rpmnew` suffix.

Citrix Integration

For Citrix integration in VMware Identity Manager 3.3, all external connectors must be version 2018.8.1.0 (the connector version in the 3.3 release) or later.

You must also upgrade to Integration Broker 3.32 or later. Upgrade is not available for Integration Broker. Uninstall the old version, then install the new version.

Troubleshooting Upgrade Errors

4

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.

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 4-1. 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	`/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`	Messages related to directory sync.
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.