Migrate to VMware Identity Manager 3.3 from AirWatch Installation (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 VMware Identity Manager for Windows 3.3

1

Beginning with VMware Identity Manager for Windows 3.2.0.1, the AirWatch installer EXE setup file no longer includes the installation of VMware Identity Manager.

A separate VMware Identity Manager EXE set up file can be downloaded from the My VMware downloads page.

Supported Upgrade Path

VMware Identity Manager 3.1 is installed as part of the AirWatch installations for AirWatch version 9.2.2 through 9.3.x.

To upgrade to version 3.3 from the AirWatch install, VMware Identity Manager must be at version 3.1.

For upgrade instructions to version 3.1, see the VMware AirWatch Upgrade Guide.

Understanding the Upgrade Process

Because the VMware Identity Manager for Windows 3.3 is a standalone installer, when you upgrade from 3.1, running the VMware Identity Manager EXE file performs the following actions.

- Migrates the VMware Identity Manager installation directory from the AirWatch directory structure to a staging directory on the server
- Uninstalls the AirWatch directory from the server
- Copies the files from the staging directory to the VMware directory
- Upgrades VMware Identity Manager

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

Migrating and Upgrading Servers in the Cluster

2

For each node in the cluster, you migrate the VMware Identity Manager 3.1 files from the AirWatch installation directory and then upgrade VMware Identity Manager for Windows. Expect some downtime during the upgrade and plan the timing of your upgrade accordingly.

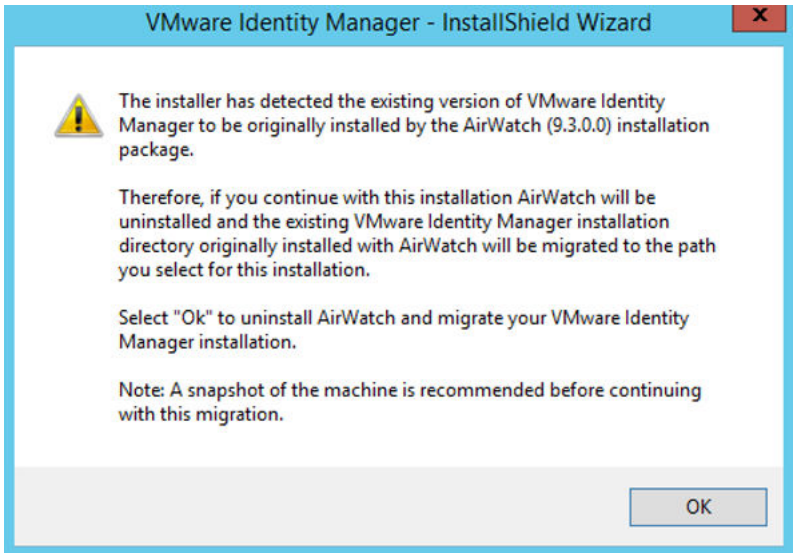
Prerequisites

- Take a snapshot of the database and the VMware Identity Manager nodes before migrating and upgrading.
- 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 Chapter 3 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 Chapter 4 Disable SQL Server AlwayOn Availability Groups Before Upgrading
- 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.



The installer detects a previous version of identity manager and asks you to select **OK** to uninstall AirWatch and migrate the VMware Identity Manager installation.

2 Select **OK**.

The VMware Identity Manager configuration directory is migrated to the local drive `vidm-migration-staging` directory.

3 To start the upgrade, click **Next**.

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

5 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.

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

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

8 In the configuration dialog box, confirm the Internal Server Hostname and port number 443 are correct and click **Next**.

9 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.

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

   During the upgrade, the following actions are performed.

   - The AirWatch directory is uninstalled.
   - The files in the `vidm-migration-staging` folder are copied to the directory created in Step 7.
   - The files in that directory are upgraded to VMware Identity Manager 3.3.

11 Click **Finish**.

The upgrade is complete and the VMware Identity Manager service is restarted.

What to do next

Upgrade the other nodes in the cluster.

If you disabled SQL Server availability groups, re-enable the availability groups. See Chapter 5 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

Add the db_owner Role Before Upgrade

3

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

4

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

5

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>;
```