Upgrading to VMware Workspace ONE Access 20.10.0.0

OCT 2020

VMware Workspace ONE Access 20.10

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

Upgrading to VMware Workspace ONE Access 20.10.0.0

You can upgrade to Workspace ONE Access 20.10 directly from either Workspace ONE Access 20.01 or VMware Identity Manager 19.03 on Linux.

Starting with version 20.01, the VMware Workspace ONE® Access™ service (formerly known as VMware Identity Manager™) is available on-premises solely on Linux. If your existing Linux deployment is a version earlier than 19.03, you must upgrade to 19.03 first.

To upgrade VMware Identity Manager 19.03 on Windows to Workspace ONE Access 20.10, do not perform the upgrade procedure. Perform the migration procedure from VMware Identity Manager 19.03 on Windows to version 20.01 on Linux first. See *Migrating Windows to Linux for VMware Workspace ONE Access 20.01*.

For existing Linux deployments, if you prefer a fresh installation to an upgrade, see *Installing and Configuring VMware Workspace ONE Access*. Remember that a new installation does not preserve your existing configurations.

Intended Audience

This information is intended for administrators of Workspace ONE Access. The information is written for experienced Linux and Windows 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 VMware ThinApp®, Citrix-published resources, and RSA SecurID, is helpful if you plan to implement those features.

Workspace ONE Access and Other Technologies

You must integrate the Workspace ONE Access service with several other technologies, including the Workspace ONE Access connector, which starting with version 19.03, is available solely on Windows. You must integrate the service with other VMware technologies, such as vCenter™, ESX™, and vSphere®. Knowledge of many other technologies is required, such as of Active Directory, databases, backup and restore procedures, Simple Mail Transfer Protocol (SMTP), and NTP servers. Knowledge of other technologies, such as VMware Horizon and RSA SecurID, is helpful if you plan to implement those features.

Overview of Upgrading to Workspace ONE Access 20.10

1

You can upgrade from earlier versions of the product to version 20.10

Product Version Numbers

This version of Workspace ONE Access is 20.10. Previous versions include 20.01, 19.03, and 3.3.

Supported Upgrade Paths

Note If you applied security patch HW-137959, make sure you follow the instructions in Security Patch Process to Follow During Upgrade before and after you perform the upgrade.

The upgrade path from 19.03 on Linux or 20.01 directly to version 20.10 is supported.

If your Linux deployment is not currently on 19.03, perform an upgrade to 19.03 first. See *Upgrading to VMware Identity Manager 19.03.0.0 (Linux)*.

For information about upgrading from VMware Identity Manager on Windows, see Upgrading to VMware Workspace ONE Access 20.10.0.0.

- You can upgrade from version 3.2.0.1 or 3.3 directly to version 19.03.0.0.
- To upgrade from a version prior to 3.2.0.1, you must first upgrade to version 3.2.0.1, and then upgrade from 3.2.0.1 to 19.03.0.0. When you perform an online upgrade, the latest version to which upgrade is permitted appears. If necessary, upgrade to the allowed version and then upgrade to 3.2.0.1. See *Upgrading to VMware Identity Manager 3.2.0.1 (Linux)* for information.

Compatibility with Workspace ONE UEM

VMware Product Interoperability Matrix provides details about the compatibility of current and previous versions of VMware products and components, such as VMware Workspace ONE UEM Console.

Internet Connectivity

You can upgrade from versions 19.03 on Linux or 20.01 online or offline.

By default, the Workspace ONE Access 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. You can either use the `updateoffline.hzn` script to perform the upgrade or set up a local Web server to host the upgrade file.

Upgrade Scenarios

- For your existing deployment, if you deployed a single Workspace ONE Access appliance, upgrade it online or offline as described in Chapter 2 Online Upgrading to Workspace ONE Access 20.10 or Chapter 3 Upgrading Workspace ONE Access Offline.

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

- For your existing deployment, 19.03 or 20.01, if you deployed multiple virtual appliances in a cluster for failover or high availability, see Upgrade a Workspace ONE Access Cluster.
- To upgrade from Workspace ONE Access with minimal downtime in a multi-data center deployment scenario, see "Upgrading Workspace ONE Access with Minimal Downtime" in *Installing and Configuring VMware Workspace ONE Access*.

This chapter includes the following topics:

- Security Patch Process to Follow During Upgrade
- Upgrade a Workspace ONE Access Cluster

Security Patch Process to Follow During Upgrade

Security patch HW-137959 is available for the following VMware Identity Manager versions, 3.3.2, 3.3.3, 3.3.4, 3.3.5 and Workspace ONE Access versions 20.01 and 20.10.

If you install the patch on any of these versions, each time you upgrade from a previous version, before you perform the upgrade, you must restore the server.xml file on the server that is being upgraded. After you upgrade, you apply a new security patch HW-137959 on the server.

Process

- Before upgrading, restore the **server.xml** file on the appliance to be upgraded.

  Log into the appliance that is being upgraded as the root user and run `CMD : mv /opt/vmware/horizon/workspace/conf/server.xml.bk /opt/vmware/horizon/workspace/conf/server.xml`

  This removes the patch and makes this version ready to upgrade to the newer version.

- Upgrade to the virtual appliance. See Chapter 2 Online Upgrading to Workspace ONE Access 20.10.
- After you upgrade, you must apply the security patch HW-137959 for that specific upgrade version. See KB article 85254 HW-137959: VMSA-2021-0016 for Workspace ONE Access, VMware Identity Manager (CVE-2021-22002, CVE-2021-22003).

Upgrade a Workspace ONE Access Cluster

For your existing deployment, if you deployed multiple 20.01 virtual appliances in a cluster for failover or high availability, you upgrade the nodes one at a time to 20.10

Expect some downtime during upgrade and plan the timing of your upgrade accordingly.

Procedure

1 Take snapshots of the database and the service nodes.

2 Remove all nodes except one from the load balancer.

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

The first nod that you update must reindex the Elasticsearch indices. When you see the warning message asking you to run the `/usr/local/horizon/update/reindexingIndices.hzn` script, select **YES**. When you upgrade the other nodes in the cluster, select **No** as the answer to this question. The reindex script is applied only on the first node.

Follow the process for an online or offline upgrade, as described in Chapter 2 Online Upgrading to Workspace ONE Access 20.10 or Chapter 3 Upgrading Workspace ONE Access Offline.

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 Workspace ONE Access 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.

Online Upgrading to Workspace ONE Access 20.10

2

You can upgrade the Workspace ONE Access virtual appliance online. The virtual appliance must be able to connect to the Internet for an online upgrade.

Prerequisites for a Workspace ONE Access Online Upgrade

Before you upgrade the Workspace ONE Access 20.01 virtual appliance online, perform the prerequisite tasks.

- Verify that at least 10 GB of free disk space (`/dev/sda`) are available on the virtual appliance. To check for the amount of free disk space, run

  ```
  parted /dev/sda unit GB print free | grep "Free Space" |tail -n 1| awk '{print $3}'
  ```

  Note After upgrading to 20.10, use the `df -k` command to check the free disk space.

- Verify that at least 4 GB of disk space are available on the primary root partition of the virtual appliance. To see the disk space, use the `df -h` command.
- Back up the virtual appliance by taking a snapshot. For information about how to take snapshots, see the vSphere documentation.
- To ensure that Elasticsearch data is not deleted, prepare Elasticsearch for the upgrade.
  - Determine if multiple instances of Elasticsearch have ever run on any of the service nodes and, if so, consolidate the data directories of the multiple instances.
    1. View the contents of the `/db/elasticsearch/horizon/nodes` directory.

       The goal is for one subdirectory named `0` to exist. If only the `0` subdirectory exists, you do not need to consolidate directories.

       If a second copy of Elasticsearch has run at any time, a second directory named `1` also exists. Continue with the steps to consolidate directories.

    2. If multiple Elasticsearch instances exist, stop Elasticsearch and verify all processes are stopped.

       For example, to stop Elasticsearch, run the following command.

       ```
       service elasticsearch stop
       ```

For example, to verify all Elasticsearch processes are stopped, run the following command.

```
ps -ef | grep elasticsearch
```

If the `grep` command shows that additional Elasticsearch processes are running, kill those processes.

3. To determine which directory within each node contains the data, search for the data in the `indices` directory of each node, such as the following directory: `/db/elasticsearch/horizon/nodes/1/indices/`.
4. Remove the directory that does not contain the data and, if necessary, rename the remaining directory.

   If the `0` directory contains the data, remove the `1` directory.

   If the `1` directory contains the data, remove the `0` directory and rename the `1` directory `0`.
5. Restart Elasticsearch.

   ```
   service elasticsearch start
   ```
6. Search the `/opt/vmware/elasticsearch/logs/horizon.log` for a message like the following:

   recovered *xx* indices into cluster_state

   The message indicates that the system can read the renamed data directory, where *xx* represents the number of directories, or indices, in the `/db/elasticsearch/horizon/nodes/0/indices/` directory.

- Remove `sysconfig.cloneprep` and `sysconfig.iamaclone` files from all cloned service nodes.

  For example, log into each service node and run the following commands as root.

  ```
  rm -f /usr/local/horizon/conf/flags/sysconfig.cloneprep
  rm -f /usr/local/horizon/conf/flags/sysconfig.iamaclone
  ```

- To shut down the entire Elasticsearch cluster, run the `service elasticsearch stop` command on each node.

  Shutting down the entire Elasticsearch cluster allows the Elasticsearch version to upgrade while preventing mismatched versions from running.
- 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.
- Add the db_owner role to the same user that was used during installation:

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

b Connect to the database instance for the service.

c 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 username.

- For information about revoking the database-level role, see Change Database-Level Roles After Upgrade to Workspace ONE Access.
- Take a snapshot or backup of the external database.
- Verify that the service is properly configured.
- Verify that the virtual appliance can resolve and reach vapp-updates.vmware.com on ports 80 and 443 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 20.10 Workspace ONE Access Appliance.
- . Run the appropriate command to check for upgrades. See Check for the Availability of a Workspace ONE Access Upgrade Online.
- Ensure that following directory space requirements are met.

Directory	Minimum Available Space
/	4 GB
Directory where you download the `dualbootupdate.tar.gz` file, if applicable	2 GB

- Download Photon Migration Support Tools from the Workspace ONE Access 20.10 download page on my.vmware.com and save the file to any directory in the service virtual appliance.

Workspace ONE Access 20.10 switches from the SUSE Linux Enterprise Server (SLES) operating system to the VMware Photon™ operating system. The Photon Migration Support Tools download contains the `dualbootupdate.tar.gz` file, which includes the Photon operating system and its packages. The upgrade process uses the `dualbootupdate.tar.gz` file when migrating the operating system from SLES to Photon.

Configure Proxy Server Settings for the 20.10 Workspace ONE Access Appliance

The Workspace ONE Access service 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.

To use a proxy server with the service, Workspace ONE Access or VMware Identity Manager, when you install the service, you configure it using the YaST utility. To upgrade the service, you must now edit the proxy server settings by running specific `vami` commands in the service virtual appliance.

Note 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.

Prerequisites

- Verify that you have the root password for the virtual appliance. See *Installing and Configuring VMware Workspace ONE Access* for information about creating passwords for administrator accounts.
- Verify that you have the proxy server information.

1 Log in to the existing version 20.10 of the service virtual appliance, as the root user.

2 Run the following command to set the proxy.

```
/opt/vmware/share/vami/vami_set_proxy proxyServer proxyPort
```

For example:

```
/opt/vmware/share/vami/vami_set_proxy proxy.mycompany.com 3128
```

3 Run the following command to verify the proxy settings.

```
/opt/vmware/share/vami/vami_proxy
```

4 If your proxy sever requires authentication, edit the `/etc/environment` configuration file and add the user name and password. For example:

```
http_proxy=http://username:password@proxy.mycompany.com:3128
```

5 Restart the Tomcat server on the service virtual appliance to use the new proxy settings.

```
service horizon-workspace restart
```

Results

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

Check for the Availability of a Workspace ONE Access Upgrade Online

If your existing service 20.10 virtual appliance, has Internet connectivity, you can check for the availability of upgrades online from the appliance.

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

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

Example

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

This chapter includes the following topics:

- Perform an Online Upgrade to Workspace ONE Access 20.10
- Perform a Workspace ONE Access Online Upgrade to a Specific Version

Perform an Online Upgrade to Workspace ONE Access 20.10

If your existing 20.10 virtual appliance has Internet connectivity, you can upgrade the appliance online.

Prerequisites

- The prerequisites listed in Prerequisites for a Workspace ONE Access Online Upgrade are verified.
- Verify that the virtual appliance is powered on and functioning.

Procedure

1 Log in to the existing Workspace ONE Access 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 an online upgrade exists.

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

4 Enter **y** to proceed with the upgrade of the Workspace ONE Access service or enter **n** to exit the upgrade.

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 Restart the virtual appliance.

```
reboot
```

7 Check the version of the upgraded appliance.

```
vamicli version --appliance
```

The new version is displayed.

8 After you upgrade all the nodes in your Workspace ONE Access deployment, use the diagnostics dashboard to monitor system information health.

a Log in to the Workspace ONE Access console.

b Select **Dashboard > System Diagnostics Dashboard**.

c If your deployment consists of more than one Workspace ONE Access appliance, select the appliance you want to monitor.

d Check the status of the various services.

For example, to check the health of the Elasticsearch service, review the **Integrated Components** section and confirm that the values for the Elasticsearch items are as expected. Therefore, the value for **Elasticsearch - Health** is **Green**, the information about the cluster nodes is accurate, and so on.

Results

The upgrade is complete.

See Chapter 4 Post-Upgrade Configuration of Workspace ONE Access.

Perform a Workspace ONE Access Online Upgrade to a Specific Version

You can perform an online upgrade of the Workspace ONE Access service to a specific version instead of the latest available version, if required.

Note To upgrade to the latest available version, see Perform an Online Upgrade to Workspace ONE Access 20.10.

Prerequisites

- Ensure that you meet the prerequisites listed in Prerequisites for a Workspace ONE Access Online Upgrade.

- 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 update the appliance to a specific version.

   ```
   /usr/local/horizon/update/configureupdate.hzn provider --url https://vapp-
   updates.vmware.com/vai-catalog/valm/vmw/5C08B358-F782-11E1-8F08-78776188709B/newVersion
   ```

   where *newVersion* is the version to which you want to upgrade.

   - To upgrade to version 3.3, use:

     ```
     /usr/local/horizon/update/configureupdate.hzn provider --url https://vapp-
     updates.vmware.com/vai-catalog/valm/vmw/5C08B358-F782-11E1-8F08-78776188709B/3.3.0.0
     ```

   - To upgrade to version 19.03, use:

     ```
     /usr/local/horizon/update/configureupdate.hzn provider --url https://vapp-
     updates.vmware.com/vai-catalog/valm/vmw/5C08B358-F782-11E1-8F08-78776188709B/19.03.0.0
     ```

   - To upgrade to version 20.01, use:

     ```
     /usr/local/horizon/update/configureupdate.hzn provider --url https://vapp-
     updates.vmware.com/vai-catalog/valm/vmw/5C08B358-F782-11E1-8F08-78776188709B/20.01.0.0
     ```

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

4. Restart the virtual appliance.

   ```
   reboot
   ```

5. Check the version of the upgraded appliance.

   ```
   vamicli version --appliance
   ```

   The new version is displayed.

6. After you upgrade all the nodes in your Workspace ONE Access deployment, use the diagnostics dashboard to monitor system information health.

   a. Log in to the Workspace ONE Access console.

   b. Select **Dashboard > System Diagnostics Dashboard**.

c If your deployment consists of more than one Workspace ONE Access appliance, select the appliance you want to monitor.

d Check the status of the various services.

For example, to check the health of the Elasticsearch service, review the **Integrated Components** section and confirm that the values for the Elasticsearch items are as expected. Therefore, the value for **Elasticsearch - Health** is **Green**, the information about the cluster nodes is accurate, and so on.

Results

The upgrade is complete.

Upgrading Workspace ONE Access Offline

3

If your Workspace ONE Access 20.01.0.0 virtual appliance cannot connect to the Internet for upgrade, you can perform an offline upgrade.

Two options are available for offline upgrade. You can set up an upgrade repository on a local Web server and configure the appliance to use the local Web server for upgrade. Or you can download the upgrade package to the Workspace ONE Access 20.01.x server and use the `updateoffline.hzn` script to upgrade.

Prerequisites for a Workspace ONE Access Offline Upgrade

Before you upgrade the Workspace ONE Access 20.01 virtual appliance offline, perform these prerequisite tasks.

- Take a snapshot of your virtual appliance to back it up. For information about how to take snapshots, see the vSphere documentation.
- Verify that at least 10 GB of free disk space (`/dev/sda`) are available on the virtual appliance. To see if you have enough disk space, run

  ```
  parted /dev/sda unit GB print free | grep "Free Space" |tail -n 1| awk '{print $3}'
  ```

- Verify the health of the Elasticsearch service Go to the System Diagnostic Dashboard in the Workspace ONE Access console and review the Integrated Components section. Confirm that the values for the Elasticsearch items are green. If the state displays as red, fix the Elasticsearch issues before upgrading.
- If you revoked the db_owner role on the Microsoft SQL database, you must add it back before performing the upgrade, otherwise the upgrade fails. Add the db_owner role to the same user that was used during installation:
  a Log in to the Microsoft SQL Server Management Studio as a user with sysadmin privileges.
  b Connect to the database instance for Workspace ONE Access 20.10
  c 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 username.

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 username.

For information about revoking the database-level role, see Change Database-Level Roles After Upgrade to Workspace ONE Access

- Take a snapshot or backup of the external database.
- Verify that Workspace ONE Access is properly configured.
- Confirm that a Workspace ONE Access upgrade exists. Check the My VMware site at my.vmware.com for upgrades.
- If you are upgrading using the `updateoffline.hzn` script and your deployment includes a proxy server, disable the proxy server.

  Disable the proxy server from the command line.

  a Run the following command.

  ```
  yast2
  ```

  The YaST2 Control Center dialog box opens.

  b Select **Network services**.

  c Select **Proxy**.

  The Proxy Configuration dialog box opens.

  d If selected, deselect **Enable proxy**.

  e Quit the YaST2 utility.

  After a successful upgrade, enable the proxy server again.

- Ensure that following directory space requirements are met.

Directory	Minimum Available Space
/	4 GB
Directory where you download the `dualbootupdate.tar.gz` file, if applicable	2 GB
Directory where you download the offline upgrade package, `identity-manager-20.10.0.0-`*`buildNumber`*`-updaterepo.zip`	2 GB

- Download Photon Migration Support Tools from the Workspace ONE Access 20.10 download page on my.vmware.com and save the file to any directory in the service virtual appliance.

  Workspace ONE Access 20.10 switches from the SUSE Linux Enterprise Server (SLES) operating system to the VMware Photon™ operating system. The Photon Migration Support Tools download contains the dualbootupdate.tar.gz file, which includes the Photon operating system and its packages. The upgrade process uses the dualbootupdate.tar.gz file when migrating the operating system from SLES to Photon.

This chapter includes the following topics:

Using a Local Web Server for a Workspace ONE Access Offline Upgrade

If you want to perform the offline upgrade using a local web server, prepare the web server to host the upgrade file, configure the existing 20.10.X Workspace ONE Access appliance to point to the web server, and perform the upgrade.

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 Workspace ONE Access virtual appliance.

Prerequisites

- Perform the general offline-upgrade prerequisites. Chapter 3 Upgrading Workspace ONE Access Offline.
- Download the VMware Workspace ONE Access offline upgrade package, `identity-manager-20.10.0.0-`*`buildNumber`*`-updaterepo.zip`, from the VMware Workspace ONE Access product download page on my.vmware.com.
- If you use Web Server (IIS), 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 Workspace ONE Access 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. See the preceding section.

Procedure

1 Log in to the Workspace ONE Access 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 Restart the virtual appliance.

```
reboot
```

e Check the version of the upgraded appliance.

```
vamicli version --appliance
```

The new version is displayed.

f After you upgrade all the nodes in your Workspace ONE Access deployment, use the diagnostics dashboard to monitor system information health.

1 Log in to the Workspace ONE Access console.

2 Select **Dashboard > System Diagnostics Dashboard**

3 If your deployment consists of more than one Workspace ONE Access appliance, select the appliance you want to monitor.

4 Check the status of the various services.

For example, to check the health of the Elasticsearch service, review the **Integrated Components** section and confirm that the values for the Elasticsearch items are as expected. Therefore, the value for **Elasticsearch - Health** is **Green**, the information about the cluster nodes is accurate, and so on.

Results

The upgrade is complete.

See Chapter 4 Post-Upgrade Configuration of Workspace ONE Access.

Using the updateoffline.hzn Script for an Offline Upgrade of Workspace ONE Access

You can use the `updateoffline.hzn` script to perform an offline upgrade of the existing service virtual appliance. Download the offline upgrade package from the VMware Workspace ONE Access product download page to use with the script.

The script verifies that the upgrade package matches the product. For example, if you are upgrading the Workspace ONE Access service virtual appliance and you use the connector upgrade package instead of the service upgrade package, the script results in an error.

Prerequisites

- Perform the general offline-upgrade prerequisites. See Prerequisites for a Workspace ONE Access Offline Upgrade.
- Download the VMware Workspace ONE Access offline upgrade package, `identity-manager-20.10.0.0-buildNumber-updaterepo.zip`, from the VMware Workspace ONE Access product download page on my.vmware.com.

  The recommended location for saving the file is `/var/tmp`.
- Verify that at least 4 GB of disk space are available on the primary root partition of the virtual appliance after copying `identity-manager-20.10.0.0-buildNumber-updaterepo.zip` to the appliance.

Procedure

1 Locate the `updateoffline.hzn` script.

  The script is available at the following path:

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

2 Run the `updateoffline.hzn` script as the root user.

  `/usr/local/horizon/update/updateoffline.hzn [-r] -f upgradeFilePath`

-f *upgradeFilePath*	Upgrade the appliance using *upgradeFilePath*. *upgradeFilePath* must be an absolute path.	Required
-r	Reboot after upgrade.	Optional
-h	Displays the script usage.	Optional

  For example:

  `/usr/local/horizon/update/updateoffline.hzn -f /var/tmp/identity-manager-20.10.0.0-buildNumber-updaterepo.zip`

3 If the "`The product RID matches so continue`" prompt appears, press **Enter** to continue.

4 If you did not use the `-r` option with the script, restart the virtual appliance after upgrade is complete.

  `reboot`

5 After you upgrade all the nodes in your Workspace ONE Access deployment, use the diagnostics dashboard to monitor system information health.

  a Log in to the Workspace ONE Access console.

  b Select **Dashboard > System Diagnostics Dashboard**.

c If your deployment consists of more than one Workspace ONE Access appliance, select the appliance you want to monitor.

d Check the status of the various services.

For example, to check the health of the Elasticsearch service, review the **Integrated Components** section and confirm that the values for the Elasticsearch items are as expected. Therefore, the value for **Elasticsearch - Health** is **Green**, the information about the cluster nodes is accurate, and so on.

Post-Upgrade Configuration of Workspace ONE Access

4

After you upgrade to Workspace ONE Access 20.10.0.0, you might need to configure certain settings.

Apply Security Patch HW-137959

After you upgrade, apply the security patch HW-137959 for this specific upgrade version. See VMware KB article 85254 HW-137959: VMSA-2021-0016 for Workspace ONE Access, VMware Identity Manager (CVE-2021-22002, CVE-2021-22003).

Configuring Workspace ONE Access Connector Instances

You can upgrade your existing Workspace ONE Access connector installation to version 20.10 to get the latest features such as the new Virtual App service, security updates, and resolved issues. Workspace ONE Access connector is a component of Workspace ONE Access. See the Installing VMware Workspace ONE Access Connector 20.10 guide.

Log4j Configuration Files

If any `log4j` configuration files in a Workspace ONE Access 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 virtual appliance.

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.

Save the Workspace ONE UEM Configuration

Saving the Workspace ONE UEM configuration populates the Device Services URL for the catalog. Perform this task to allow new end users to enroll and manage their devices.

1 Log in to the Workspace ONE Access console.

2 Select **Identity & Access Management > Setup > VMware Workspace ONE UEM**.

3 In the Workspace ONE UEM Configuration section, click **Save**.

Cluster ID in Secondary Data Center

Cluster IDs are used to identify the nodes in a cluster.

If your Workspace ONE Access 20.10 deployment includes a secondary data center, you might need to change the cluster ID of the secondary data center after upgrade.

Workspace ONE Access detects and assigns a cluster ID automatically when a new service appliance is powered up. For a multiple data center deployment, each cluster must be identified with a unique ID.

All appliances that belong to a cluster have the same cluster ID and a cluster typically consists of three appliances.

When you set up the secondary data center, verify that the cluster ID is unique to the data center. If a cluster ID is not unique to the data center, verify that each node has the Elasticsearch discovery-idm plugin installed and edit the cluster ID manually as described in the instructions that follow. You only need to perform these actions once and only on the secondary data center.

1 Verify that each node has the Elasticsearch discovery-idm plugin.

   a Log in to the virtual appliance.

   b Use the following command to check if the plugin is installed.

   ```
   /opt/vmware/elasticsearch/bin/plugin list
   ```

   c If the plugin does not exist, use the following command to add it.

   ```
   /opt/vmware/elasticsearch/bin/plugin install file:///opt/vmware/
   elasticsearch/jars/discovery-idm-1.0.jar
   ```

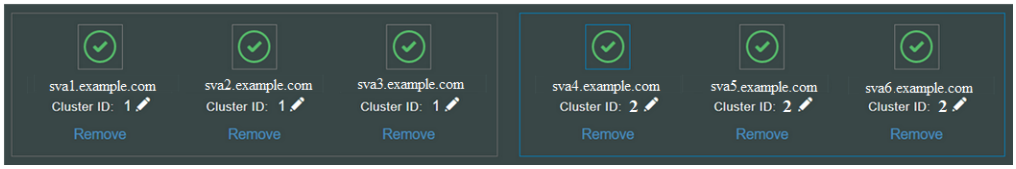
2 Log in to the Workspace ONE Access console.

3 Select the **Dashboard > System Diagnostics Dashboard** tab.

4 In the top panel, locate the cluster information for the secondary data center cluster.

5 Update the cluster ID of all the nodes in the secondary data center to a different number than the one used in the first data center.

   For example, set all the nodes in the secondary data center to 2, if the first data center is not using 2.



6 Verify that the clusters in both the primary and secondary data centers are formed correctly.

Follow these steps for each node in the primary and secondary data centers.

a Log in to the virtual appliance.

b Run the following command:

```
curl 'http://localhost:9200/_cluster/health?pretty'
```

If the cluster is configured correctly, the command returns a result similar to the following example:

```
{
  "cluster_name" : "horizon",
  "status" : "green",
  "timed_out" : false,
  "number_of_nodes" : 3,
  "number_of_data_nodes" : 3,
  "active_primary_shards" : 20,
  "active_shards" : 40,
  "relocating_shards" : 0,
  "initializing_shards" : 0,
  "unassigned_shards" : 0,
  "delayed_unassigned_shards" : 0,
  "number_of_pending_tasks" : 0,
  "number_of_in_flight_fetch" : 0
}
```

Cache Service Setting in Secondary Data Center Appliances

If you set up a secondary data center, Workspace ONE Access instances in the secondary data center are configured for read-only access with the `"read.only.service=true"` entry in the `/usr/local/horizon/conf/runtime-config.properties` file. After you upgrade such an appliance, the service fails to start.

To resolve this issue, perform the steps that follow. The steps include an example scenario of a secondary data center containing the following three nodes.

sva1.example.com
sva2.example.com
sva3.example.com

1 Log in to a virtual appliance in the secondary data center as the root user.

For this example, log in to `sva1.example.com`.

2 Edit the `/usr/local/horizon/conf/runtime-config.properties` file as indicated in the substeps that follow.

You might be able to edit an existing entry, or you can add a new entry. If applicable, uncomment entries that are commented out.

a Set the value of the `cache.service.type` entry to `ehcache`.

```
cache.service.type=ehcache
```

b Set the value of the `ehcache.replication.rmi.servers` entry to the fully qualified domain names (FQDN) of the other nodes in the secondary data center. Use a colon `:` as the separator.

For this example, configure the entry as follows.

```
ehcache.replication.rmi.servers=sva2.example.com:sva3.example.com
```

3 Restart the service.

```
service horizon-workspace restart
```

4 Repeat the preceding steps on the remaining nodes in the secondary data center.

For this example, the remaining nodes to configure are `sva2.example.com` and `sva3.example.com`.

Citrix Integration

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

You must also use Integration Broker 3.3. Upgrade is not available for Integration Broker. Uninstall the old version, then install the new version.

Troubleshooting Workspace ONE Access Upgrade Errors

5

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

This chapter includes the following topics:

Checking the Workspace ONE Access 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, Workspace ONE Access does not start and errors appear in the error logs.

Cause

Errors occurred during upgrade.

Solution

1. Log in to the Workspace ONE Access 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 the Original Workspace ONE Access Instance

If Workspace ONE Access 20.10 does not start properly after an upgrade, you can roll back to the 20.01 instance of the service.

Problem

After you upgrade Workspace ONE Access, 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 service instance and external database, if applicable. For information, see the vSphere documentation.

Collecting a Workspace ONE Access Log File Bundle

You can collect a bundle of log files. You obtain the bundle from the Workspace ONE Access 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 (Workspace ONE Access connector log files are stored in the connector server. See information about Workspace ONE Access connector log files and bundles in the latest *Installing VMware Workspace ONE Access Connector* guide.)	`/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.

Table 5-1. Log Files (continued)

Component	Location of Log File	Description
Service Logs (horizon.log)	`/opt/vmware/horizon/workspace/logs/horizon.log`	The service log records activity that takes place on the Workspace ONE Access 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 Workspace ONE Access appliance configuration page at https://*WS1AccessHostnameFQDN*:8443/cfg/logs.
2. Click **Prepare log bundle**.
3. Download the bundle.

Networking Error after Workspace ONE Access Upgrade

After you upgrade the virtual appliance and reboot, a networking error occurs.

Problem

After you upgrade the appliance, the following error message appears:

```
NO NETWORKING DETECTED. PLEASE LOGIN AND RUN THE COMMAND
/opt/vmware/share/vami/vami_config_net TO CONFIGURE THE NETWORK
```

Solution

1. Roll back to the snapshot you created before upgrading the virtual appliance.
2. Either log in to the virtual appliance as the root user or log in as the sshuser and run the `su` command to switch to super user.
3. Navigate to the following directory:

   `/etc/sysconfig/networking/devices`
4. Back up the `ifcfg-eth0` file to another directory.
5. Upgrade the virtual appliance but do not restart it.
6. Restore the `ifcfg-eth0` file to the `/etc/sysconfig/networking/devices` directory.
7. Restart the virtual appliance:

   `reboot`

Chain Workspace ONE Access Upgrade Fails During the Preupdate Process

A chain upgrade creates multiple instances of the `bc-fips-1.0.x.BC-FIPS-Certified.jar` file, which causes an upgrade to fail during the preupdate process.

Problem

When you try to upgrade to Workspace ONE Access, the following error message appears and the upgrade aborts.

```
Please validate database permissions and try upgrade again
The pre-update process failed, upgrade aborted.
```

Cause

Performing a series of Workspace ONE Access upgrades might result in the creation of a `bc-fips-1.0.0.BC-FIPS-Certified.jar` file and a `bc-fips-1.0.1.BC-FIPS-Certified.jar`. The existence of both files at the same time causes the upgrade to fail.

Solution

1. Go to the `/usr/local/horizon/jre-endorsed/` directory.
2. If both the `bc-fips-1.0.0.BC-FIPS-Certified.jar` file and the `bc-fips-1.0.1.BC-FIPS-Certified.jar` exist, delete the older version, `bc-fips-1.0.0.BC-FIPS-Certified.jar`, and perform the upgrade again.

Workspace ONE Access Upgrade Results in a Harmless NullPointerException Error

An upgrade of a Workspace ONE Access deployment might result in a NullPointerException error message.

Problem

When you issue the `/usr/local/horizon/update/updatemgr.hzn update` command, the command output might include a java.lang.NullPointerException error.

Solution

1. Ignore the NullPointerException error message.

   The upgrade succeeds as indicated at the end of the command output.
2. Proceed to reboot the virtual appliance as instructed.