Upgrading to VMware Workspace ONE Access 23.09

SEPTEMBER 2023

VMware Workspace ONE Access 23.09

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

Overview of Upgrading to VMware Workspace ONE Access 23.09

1

You upgrade to VMware Workspace ONE® Access™ 23.09 directly from Workspace ONE Access 22.09.X.

For existing 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.

Supported Upgrade Paths

To upgrade to Workspace ONE Access 23.09, the current version must be Workspace ONE Access 22.09.X.

Note The table lists the versions that can be upgraded in Workspace ONE Access.

From Workspace ONE Access Version	Upgrade to Version
22.09. or 22.09.1.0	23.09.0.0

Additionally, legacy connectors (version 19.03.0.1 and earlier) are not compatible with Workspace ONE Access virtual appliance version 23.09. You must migrate your legacy connectors to 22.09.x (or an earlier, supported version of the enterprise connector) before upgrading your Workspace ONE Access virtual appliances to 23.09.

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.

Product Version Number

When the upgrade is complete, the new version of Workspace ONE Access is 23.09.

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 version 22.09.X to version 23.09 using either online or offline upgrade methods.

By default, the Workspace ONE Access appliance uses the VMware web site for the upgrade procedure. This method 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 Process Options from Workspace ONE Access 22.09.X

- 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 23.09 or Chapter 3 Upgrading Workspace ONE Access Offline to 23.09.

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

- For your existing deployment of 22.09.X, 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*.

Read the following topics next:

- Upgrade a Workspace ONE Access Cluster

Upgrade a Workspace ONE Access Cluster

For your existing Workspace ONE Access deployment, if you deployed multiple 22.09.X virtual appliances in a cluster for failover or high availability, you upgrade the nodes one at a time to 23.09.

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

Procedure

1. Take snapshots of the database and the service nodes. See KB article 2032907, Managing snapshots in vSphere Web Client.
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 Online Upgrading to Workspace ONE Access 23.09 or Chapter 3 Upgrading Workspace ONE Access Offline to 23.09.
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 23.09

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 22.09.X virtual appliance online, perform these prerequisite tasks.

- 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, run the `df -h` command.
- Back up the virtual appliance by taking a snapshot. For information about how to take a snapshot. See KB article 2032907, Managing snapshots in vSphere Web Client.
- Microsoft SQL server 2014 updated with the Microsoft SQL patch to support TLS1.2.
- 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:
  - 1 Log in to the Microsoft SQL Server Management Studio as a user with sysadmin privileges.
    2 Connect to the database instance for the service.
    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.

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 before upgrading 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 is met.

Directory	Minimum Available Space
/	4 GB

- Make sure all connectors in your deployment are version 22.09.x or an earlier, supported version of the enterprise connector

  Legacy connectors (version 19.03.0.1 and earlier) are not compatible with Workspace ONE Access virtual appliance version 23.09. Migrate your legacy connectors to 22.09.x (or an earlier, supported version of the enterprise connector) before upgrading your Workspace ONE Access virtual appliances to 23.09. After upgrading the virtual appliances to 23.09, upgrade the connectors to 23.09.

  See Migrating to VMware Workspace ONE Access Connector 22.09 or Upgrading to VMware Workspace ONE Access Connector 22.09.

Configure Proxy Server Settings before upgrading Workspace ONE Access Appliance

The Workspace ONE Access 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.

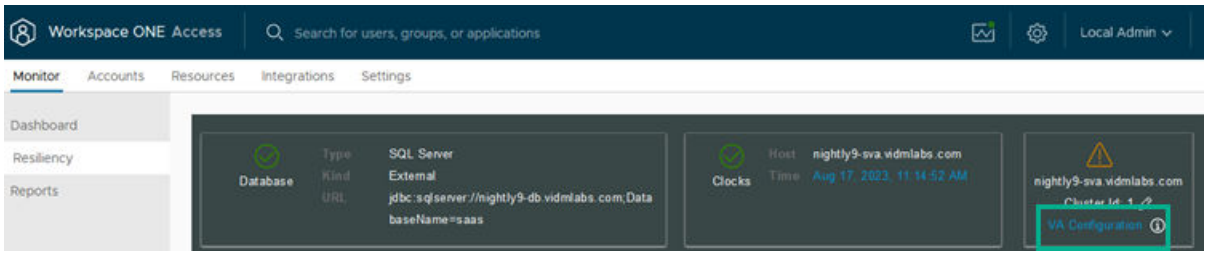
Enable your proxy to handle internet traffic only. To ensure that the proxy is set up correctly, in the Workspace ONE Access service version 22.09 set the parameter for internal traffic to **no-proxy** within the domain.

Prerequisites

- Verify that you have the proxy server information.

1 Log in to the Workspace ONE Access console and select **Monitor > Resiliency**.

2 Click **VA Configuration** for the service node that with the proxy server information configured. The VA configurator page opens.



3 Click **Proxy Configuration**.

4 Enable **Proxy**.

5 In the **Proxy host with port** text box, enter the proxy name and port number. For example, **`proxyhost.example.com:3128`**.

6 In the **Non-Proxied hosts** text box, enter the non-proxy hosts that are accessed without going through the proxy server.

Use a comma to separate a list of host names.

7 Click **Save**.

Results

The VMware update servers are now available to the Workspace ONE Access virtual appliance.

Check for the Availability of a Workspace ONE Access Upgrade Online

If your existing Workspace ONE Access 22.09.X 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.

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

Read the following topics next:

- Perform an Online Upgrade to Workspace ONE Access 23.09
- Perform a Workspace ONE Access Online Upgrade to a Specific Version

Perform an Online Upgrade to Workspace ONE Access 23.09

If your existing 22.09.X 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.
- For Workspace ONE Access 23.09, the Mobile SSO CertProxy configuration page UI was redesigned. If you enabled the VA-Configuration > Mobile SSO > Android SSO cert proxy settings in your environment, during the upgrade, you are asked to update the following CertProxy settings.
  - Number of load balancers. Enter the number of load balancers that are between the CertProxy service and the Workspace ONE Access instance or enter 0 if a load balancer is not used.
  - Client IP load balancer header name (Remote IP source). This is the source used to obtain the CertProxy instance IP from the HTTP request. The value can be **X-forwarded-For** header or **X-Real-Ip** header. If the number of load balancers is 0, Remote IP source is automatically set to **Request remote address**.
  - The allowlist of CertProxy instance IP addresses to accept authentication requests from. The current IP addresses configuration is pre-populated. You can make changes or click **Enter** to keep the current configuration. To change the allowlist, enter IP addresses of CertProxy instances separated by a semicolon, either in CIDR format, subnet format delimited by a space, or as a single IP.

    Important If the number of load balancers is 0 and the CertProxy destination is set to localhost, you must add the localhost IP to the list of IP addresses in the allowlist. This is usually 127.0.0.1.

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 Run the following command to update the appliance.

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

a If the CertProxy service is enabled, the following settings must be updated.

1 `Please provide number of load balancers between CertProxy and Access instance:`

Note If you do not use a load balancer, enter **0** as the value. When you enter 0, the next CertProxy question does not display.

2 `Please provide client IP load balancer header name (x-forwrded-for/x-real-ip):`

3 `Please provide list of CertProxy instance IP addresses, separated by a semicolon, either in CIDR format, subnet format delimited by a space, or as a single IP:`

Important If the number of load balancers is 0 and the CertProxy destination is set to localhost, you must add the localhost IP to the list of IP addresses in the allowlist. This is usually 127.0.0.1.

b When asked `Would like to execute script /usr/local/horizon/update/reindexingIndices.hzn?`, enter **y** when you upgrade the first node in a cluster. When you upgrade the other nodes in the cluster, enter **n**.

For a single node upgrade, the setting is **y** by default.

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 **Monitor > Resiliency** to open the 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 OpenSearch service, review the **Integrated Components** section and confirm that the values for the OpenSearch items are as expected. Therefore, the value for **OpenSearch - Health** is **Green**, the information about the cluster nodes is accurate, and so on.

Results

The upgrade is complete.

For tasks that might need to be performed after the upgrade to 23.09, 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 23.09.

Prerequisites

- Ensure that you meet the prerequisites listed in appropriate version of the upgrade guide. You can access the upgrade guides from the Workspace ONE Access documentation center.
- Verify that the virtual appliance is powered on and functioning.

Procedure

1 Log in to the 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 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 21.08.0.1 use:

```
/usr/local/horizon/update/configureupdate.hzn provider --url https://vapp-
updates.vmware.com/vai-catalog/valm/vmw/5C08B358-F782-11E1-8F08-78776188709B/21.08.0.1
```

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. Enter `reboot`.

5 Check the version of the upgraded appliance. Enter `vamicli version --appliance`.

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 **Monitor > Resiliency** to open the 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 OpenSearch service, review the **Integrated Components** section and confirm that the values for the OpenSearch items are as expected. Therefore, the value for **OpenSearch - Health** is **Green**, the information about the cluster nodes is accurate, and so on.

Results

The upgrade is complete.

Upgrading Workspace ONE Access Offline to 23.09

3

If your Workspace ONE Access 22.09.X 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 22.09.X server and use the `updateoffline.hzn` script to upgrade.

Prerequisites for a Workspace ONE Access Offline Upgrade

Before you upgrade the 22.09.X virtual appliance to 23.09.X offline, perform these prerequisite tasks.

- Take a snapshot of your virtual appliance to back it up. For information about how to take snapshots. See KB article 2032907, Managing snapshots in vSphere Web Client.
- Microsoft SQL server 2014 updated with the Microsoft SQL patch to support TLS 1.2.
- 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 22.09.X
  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 user name.

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, deactivate the proxy server.

  Deactivate the proxy server from the Workspace ONE Access console.

  a Log in to the Workspace ONE Access console and navigate to the **Monitor > Resiliency** page.

  b Select the appliance and click **VA Configuration**.

  c Click **Manage Configuration**, log in with the admin user password, and click **Proxy Configuration**.

  d Deactivate **Proxy**.

  e Click **Save**.

  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 offline upgrade package, `identity-manager-23.09.0.0-`*`buildNumber`*`-updaterepo.zip`	2 GB

- Make sure all connectors in your deployment are version 22.09.x or an earlier, supported version of the enterprise connector

  Legacy connectors (version 19.03.0.1 and earlier) are not compatible with Workspace ONE Access virtual appliance version 23.09. Migrate your legacy connectors to 22.09.x (or an earlier, supported version of the enterprise connector) before upgrading your Workspace ONE Access virtual appliances to 23.09. After upgrading the virtual appliances to 23.09, upgrade the connectors to 23.09.

See Migrating to VMware Workspace ONE Access Connector 22.09 or Upgrading to VMware Workspace ONE Access Connector 22.09.

Read the following topics next:

- Using a Local Web Server for a Workspace ONE Access Offline Upgrade to 23.09
- Using the updateoffline.hzn Script for an Offline Upgrade of Workspace ONE Access to 23.09

Using a Local Web Server for a Workspace ONE Access Offline Upgrade to 23.09

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 22.09.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.

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

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 to the VMware Workspace ONE Access appliance. Download `identity-manager-23.09.0.0-`*`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 to be used 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.

- For Workspace ONE Access 23.09, the Mobile SSO CertProxy configuration page UI was redesigned. If you enabled the VA-Configuration > Mobile SSO > Android SSO cert proxy settings in your environment, during the upgrade, you are asked to update the following CertProxy settings.
  - Number of load balancers. Enter the number of load balancers that are between the CertProxy service and the Workspace ONE Access instance or enter 0 if a load balancer is not used.
  - Client IP load balancer header name (Remote IP source). This is the source used to obtain the CertProxy instance IP from the HTTP request. The value can be **X-forwarded-For** header or **X-Real-Ip** header. If the number of load balancers is 0, Remote IP source is automatically set to **Request remote address**.
  - The allowlist of CertProxy instance IP addresses to accept authentication requests from. The current IP addresses configuration is pre-populated. You can make changes or click **Enter** to keep the current configuration. To change the allowlist, enter IP addresses of CertProxy instances separated by a semicolon, either in CIDR format, subnet format delimited by a space, or as a single IP.

    Important If the number of load balancers is 0 and the CertProxy destination is set to localhost, you must add the localhost IP to the list of IP addresses in the allowlist. This is usually 127.0.0.1.

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
```

1 If the CertProxy service is enabled, the following settings must be updated.

a `Please provide number of load balancers between CertProxy and Access instance:`

Note If you do not use a load balancer, enter **0** as the value. When you enter 0, the next CertProxy question does not display.

b `Please provide client IP load balancer header name (x-forwrded-for/x-real-ip):`

c `Please provide list of CertProxy instance IP addresses, separated by a semicolon, either in CIDR format, subnet format delimited by a space, or as a single IP:`

Important If the number of load balancers is 0 and the CertProxy destination is set to localhost, you must add the localhost IP to the list of IP addresses in the allowlist. This is usually 127.0.0.1.

2 Run the following command to update the indices. When you upgrade the nodes in a cluster, in the first node that you upgrade, enter **y** to reindex the indices. When you upgrade the other nodes in the cluster, enter **n**. For a single node upgrade, the setting is **y** by default.

```
/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`.

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

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

c Restart the virtual appliance.

```
reboot
```

d Check the version of the upgraded appliance.

```
vamicli version --appliance
```

The new version is displayed.

e 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 **Monitor > Resiliency**

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. Review each of the sections.

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 to 23.09

You can use the `updateoffline.hzn` script to perform an offline upgrade of the existing Workspace ONE Access 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 virtual appliance and you use the connector upgrade package instead of the Workspace ONE Access 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-23.09.0.0-`*`buildNumber`*`-updaterepo.zip` to the VMware Workspace ONE Access appliance. Go to the VMware Customer Connect Downloads page and scroll to VMware Workspace ONE Access in the Desktop & End-User Computing section. Click **Download Product**.

  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-23.09.0.0-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. When you upgrade nodes in a cluster, in the first node that you upgrade, enter **y** to reindex the indices. When you upgrade the other nodes in the cluster, enter **n**. For a single node upgrade, the setting is **y** by default.	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-23.09.0.0-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 the 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 **Monitor > Resiliency**.

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.

Post-upgrade Configuration of Workspace ONE Access 4

After you upgrade to Workspace ONE Access 23.09.X, review the post-upgrade configuration procedures and determine which ones you must do to complete the upgrade to 23.09.X.

Configuring Workspace ONE Access Connector Instances

You can upgrade your existing Workspace ONE Access connector installation to version 23.09 to get the latest features, security updates, and fixed resolved issues. Workspace ONE Access connector is a component of Workspace ONE Access. See the Installing VMware Workspace ONE Access Connector 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. 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

After you upgrade the appliance, you must go to the Workspace ONE Access console and save the Workspace ONE UEM configuration settings. 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 Open the **Integrations > UEM Integration** page.

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.

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, 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 Log in to the Workspace ONE Access console.

2 Select the **Monitor > Resiliency** tab.

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

4 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.

5 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.

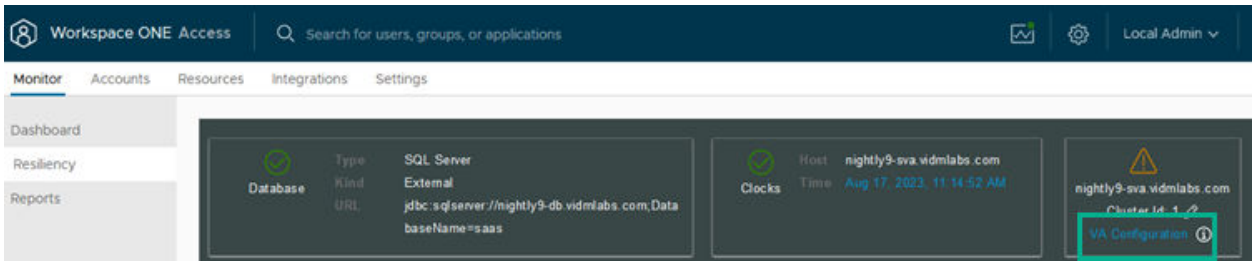
  ```
  service horizon-workspace restart
  ```

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

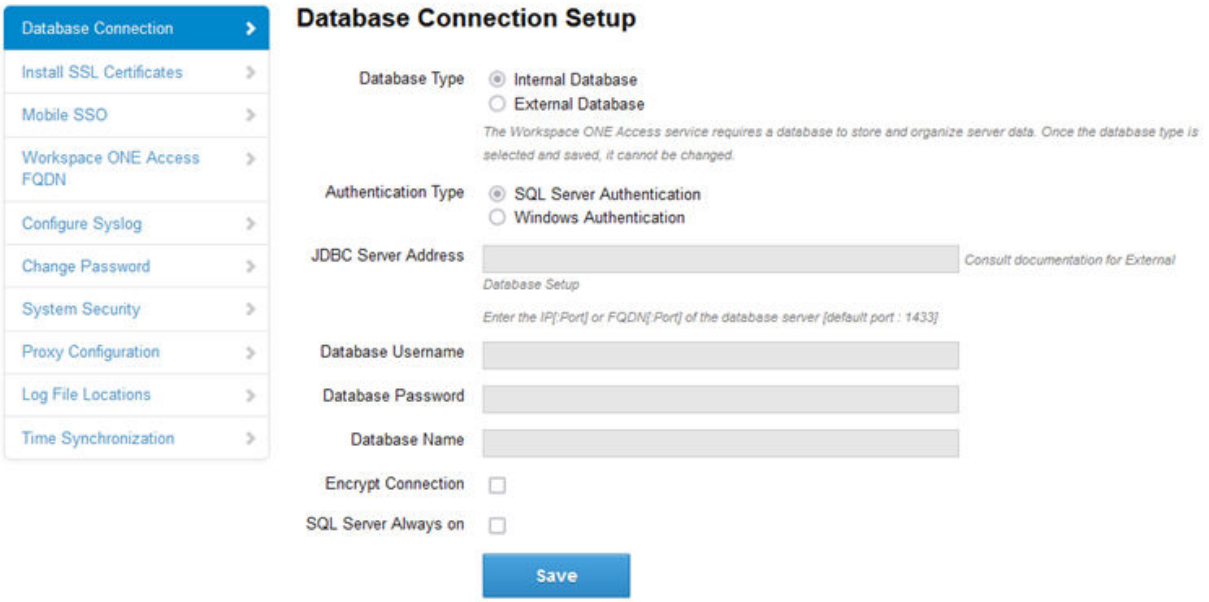
For this example, the remaining nodes to configure are `sva2.example.com` and `sva3.example.com`.

Manage External Database Properties from Workspace ONE Access Console

After an upgrade, you manage the external database properties from the Workspace ONE Access appliance VA Configuration > Database Connection Setup page. You can access this page from the Workspace ONE Access console Monitor > Resiliency page. Click VA Configuration for the service node you want to review.



The Database Connection Setup page is displayed.



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.

Read the following topics next:

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 23.09 does not start properly after an upgrade, you can roll back to the 22.09.X 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, Revert a Virtual Machine Snapshot.

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/cfg/workspace/logs	Requests that the Configurator receives from the REST client and the Web interface.
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/systemd/network and file is: 10-eth0.network`

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.