Upgrading Horizon Workspace

Horizon Workspace 1.8

This document supports the version of each product listed and supports all subsequent versions until the document is replaced by a new edition. To check for more recent editions of this document, see http://www.vmware.com/support/pubs.

EN-001323-00

You can find the most up-to-date technical documentation on the VMware Web site at:

http://www.vmware.com/support/

The VMware Web site also provides the latest product updates.

If you have comments about this documentation, submit your feedback to:

docfeedback@vmware.com

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

Contents

About Upgrading Horizon Workspace 1

The VMware® Horizon Workspace™ upgrade guide describes how to upgrade from version 1.5 to 1.8. If you have version 1.5 of Horizon Workspace and you would rather perform a fresh installation of Horizon Workspace 1.8, see *Installing and Configuring Horizon Workspace Guide*. Remember that a new installation will not preserve your existing configurations.

The update procedure requires connectivity to an update website. By default, Horizon Workspace uses the VMware website and requires Internet connectivity. See Chapter 2, "Prepare to Upgrade to Horizon Workspace 1.8," on page 7 for prerequisites.

CAUTION Upgrading from Horizon Workspace 1.0 to Horizon Workspace 1.8 is not supported. You must upgrade from Horizon Workspace 1.0 to Horizon Workspace 1.5 to Horizon Workspace 1.8.

To learn how to use and maintain your updated Horizon Workspace instance, see the *Horizon Workspace Administrator's Guide*.

Prepare to Upgrade to Horizon Workspace 1.8

2

Before you start the upgrade process, you must prepare your environment, including meeting the prerequisites, backing up your existing Horizon Workspace instance, and checking for available updates.

You run the upgrade command for Horizon Workspace 1.8 on the configurator-va virtual machine and from the command line. The upgrade command (`updatemgr.hzn`) retrieves a file that starts the upgrade. During the upgrade, each virtual machine is upgraded individually in random order. Based on the size of each virtual machine, the upgrade time varies. Because of its size, the data-va virtual machine upgrade takes the most time. When the upgrade is complete, you must manually restart the vApp by powering it off and powering it back on.

Prerequisites

- Verify that at least 2GBs of disk space is available for the upgrade to Horizon Workspace 1.8.
- Verify that Horizon Workspace is installed and properly configured.
- Take a snapshot of the vApp to back it up. For information about how to take a snapshot, see vSphere documentation.
- Back up the database if you are using an external database.
- Verify that Horizon Workspace can resolve and reach *vapp-updates.vmware.com* on port 80 over HTTP.
- If you do not have Internet connectivity, you must perform the following tasks to set up an internal Web server to use as an update server.
  - If you cannot connect to the Internet during the upgrade process, you must set up your vApp as a local Web server. See "Prepare a Local Web Server," on page 8.
  - Configure the vApp. See "Configure the vApp to Use a Local Web Server," on page 8.
  - If you use a proxy server to access the Internet, configure all virtual machines to use a proxy server before you start the update process. See "Configure the Proxy Server Settings for Virtual Machines," on page 9.

Procedure

1 Go to the configurator-va virtual machine and open the command line to check for Horizon Workspace upgrades.

2 Run the `updatemgr.hzn` command to check for the available upgrades online. You can run the upgrade command without the `check` parameter to install the upgrades.

```
/usr/local/horizon/lib/menu/ updatemgr.hzncheck
```

What to do next

If necessary, prepare a local Web server or configure proxy server settings.

This chapter includes the following topics:

- "Prepare a Local Web Server," on page 8
- "Configure the vApp to Use a Local Web Server," on page 8
- "Configure the Proxy Server Settings for Virtual Machines," on page 9

Prepare a Local Web Server

If you cannot connect to the Internet during the upgrade, you must set up an upgrade repository on a local Web server. Before you begin to upgrade Horizon Workspace, you must set up the Web server by creating a directory structure that includes five subdirectories. Each subdirectory corresponds with one of the five virtual machines.

Procedure

1 Create a directory on the Web server at http://*yourhost*/*vapp*/.

2 Create one subdirectory for each ZIP file.

Zip File	Subdirectory	Virtual Machine
`connector-1.8.0.0-1385196-updaterepo.zip`	/conn	connector-va
`configurator-va-1.8.0.0-1385195-updaterepo.zip`	/cfg	configurator-va
`gateway-va-1.8.0.0-1385192-updaterepo.zip`	/gty	gateway-va
`service-va-1.8.0.0-1385242-updaterepo.zip`	/srv	service-va
`horizon-data-va-1.8.0.0-1385194-updaterepo.zip`	/dta	data-va

3 Unzip each file into its associated directory.

Each directory contains two subdirectories: `/manifest` and `/package-pool`.

4 Run the `updatelocal.hzn` command to check that a URL has valid update contents.

```
/usr/local/horizon/lib/menu/updatelocal.hzn checkurl http://yourhost/vapp
```

Configure the vApp to Use a Local Web Server

Set up your vApp as a local Web server to update to Horizon Workspace 1.8 if you will not have Internet access during the upgrade.

Prerequisites

- If you cannot connect to the Internet during the upgrade process, set up an upgrade repository on a local Web server. "Prepare a Local Web Server," on page 8.
- If you use a proxy server to connect to the Internet, configure the proxy server settings. See "Configure the Proxy Server Settings for Virtual Machines," on page 9.

Procedure

1 Run the `updatelocal.hzn` command, on the configurator-va virtual machine, to configure an upgrade repository to use a local Web server.

```
/usr/local/horizon/lib/menu/updatelocal.hzn seturl http://yourhost/vapp
```

2 (Optional) To undo the configuration and restore the default Web server, run the `updatelocal.hzn` command.

```
/usr/local/horizon/lib/menu/updatelocal.hzn setdefault
```

What to do next

Continue with the update process.

Configure the Proxy Server Settings for Virtual Machines

Horizon Workspace Manager (service-va) virtual machines access the global catalog and other Web services on the Internet. If your network configuration provides Internet access through an HTTP proxy, you must adjust your proxy settings on the Manager (service-va) virtual machine.

Prerequisites

Verify that you know the global root password. See *Installing and Configuring Horizon Workspace Guide*.

Procedure

1 Log in as root to the Manager (service-va) virtual machine.

2 Run the YaST utility from the service-va command line.

3 Click the **Network Services** tab in the left navigation and click the **Proxy** page.

4 Type the correct proxy URL in the HTTP text box.

The global catalog and other Web services are now available to Horizon Workspace.

Upgrade to Horizon Workspace 1.8 3

You run the upgrade command from the command line on the configurator-va virtual machine. If the upgrade process is interrupted while it is in progress, when you run it again, the process resumes from where it stopped. During the upgrade, all Horizon Workspace services are stopped, so plan the upgrade with the expected downtime in mind.

Prerequisites

Go to the configurator-va virtual machine and open the command line.

Procedure

1 Run the `updatemgr.hzn` command.

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

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

2 When you upgrade an Horizon Workspace 1.5 deployment that includes multiple service-va virtual machines to Horizon Workspace 1.8, set up Horizon Workspace using these steps.

a From the command line of one of the service-va virtual machines, copy the `/usr/local/horizon/bin/masterkeys.uber` file from one of the service-va virtual machines to all of the service-va virtual machines in your deployment.

You can copy the `masterkeys.uber` file from any service-va instance if the `masterkeys.uber` file is exactly the same on every service-va virtual machine.

b Restart the appropriate servers.

c If you perform these steps after you upgrade to Horizon Workspace 1.8, run the `service horizon-frontend start` command on each service-va virtual machine where you copied the `masterkeys.uber` file.

This command restarts the front-end Web application.

3 Configure the `vami` properties in the vApp for each virtual machine in your environment.

- vami.DNSO.[virtualmachinename]
- vami.ip0.[virtualmachinename]
- vami.gateway0. [virtualmachinename]

- vami.netmask0.[virtualmachinename]

NOTE Before you upgrade, if you have more than one instance of any virtual machine type, you must configure these properties for all additional instances. The original instance installs these properties automatically.

If you add a virtual machine using the `addvm` command in the future, the `vami` properties are automatically configured.

a Power off the vApp.

NOTE You cannot edit the property settings while the vApp is running.

b Select the vApp whose properties you want to edit.

c Right-click the vApp and select **Edit Settings**.

d Click the **Options** tab.

e Click **Advanced** in the left navigation and click the **Properties** button.

f Click the **New** button and type the `vami` properties.

Option	Description
Category	Select **Networking Properties**.
Label	(Optional) Type a description of the property.
Class ID	Select **vami**.
ID	Type the Property Type: **`DNSO`**, **`ipO`**, **`gateway0`**, or **`netmask0`**.
Instance ID	Type the virtual server name.
Description	(Optional)
Expression	For the ip0 property, select the **Static Property** radio button. 1 Select **vApp IP address** from the Type drop-down menu. 2 Accept the default value for the Length field. For the DNSO, Gateway, or Netmask property, select the **Dynamic Property** radio button. 1 For DNSO, select **DNS Servers** from the Macro drop-down menu. 2 For Netmask, select **Netmask** from the Macro drop-down menu. 3 For Gateway, leave the Macro field blank. 4 Select the network that you want the virtual machine to connect to from the Network drop-down menu.
Type	This type is used if the ID is ip0.
Default Value	This type is used if the ID is ip0.
User Configurable	This type is used if the ID is ip0.

g Repeat these steps for the `vami` properties until all the virtual machines in the vApp are configured.

You have completed the vApp settings configuration.

4 On each Horizon Workspace virtual machine, create the `vm.ip` custom property.

a Select the virtual machine whose properties you want to edit.

b Right-click the virtual machine and select **Edit Settings**.

c Click the **Options** tab.

d In the left navigation, click **Advanced** under vApp Options, and click the **Properties** button.

e Click the **New** button and type the `vm.ip` property.

Option	Description
Class ID	Type **`vm`**.
ID	Type **`ip`**.
Type	To edit the `vm.ip` property, click the **Edit** link by the Type text box. 1 Select the **Dynamic Property** radio button. 2 Select **Property** from the Macro drop-down menu. 3 Select the vami.ip0 configurator-va virtual machine.
User Configurable	Check the **User Configurable** check box.

5 On each Horizon Workspace virtual machine, create the `vm.vmname` custom property.

a Right-click the virtual machine and select **Edit Settings**.

b Click the **Options** tab.

c In the left navigation, click **Advanced** under vApp Options and click the **Properties** button.

d Click the **New** button and type the `vm.vmname` properties.

Option	Description
Class ID	Type **`vm`**.
ID	Type **`vmname`**.
Type	To edit the `vm.vmname` property, click the **Edit** link by the Type text box. 1 Select the **Static Property** radio button. 2 Select **String** from the Type drop-down menu. 3 Accept the default value for the Length field.
Default Value	Type the virtual machine name, for example, **`configurator-va`**.
User Configurable	Deselect the check box.

6 Power on the vApp from vCenter.

If you might require a new data-va virtual machine in the future, you must create a datava-template after the upgrade. See the *Installing and Configuring Horizon Workspace Guide*.

7 When the upgrade is finished, run the `libreoffice-installer.sh` script on each data-va virtual machine in your deployment to upgrade from LibreOffice 3.5.6 to LibreOffice 4.0.2. See the VMware Product Interoperability Matrixes at http://www.vmware.com/resources/compatibility/sim/interop_matrix.php to verify version information.

NOTE See the *Installing and Configuring Horizon Workspace Guide* for information on installing LibreOffice Preview.

The Horizon Workspace upgrade is complete.

What to do next

Review the information about configuring Horizon Workspace after an upgrade. If necessary, you can add a buffer disk, update VMware Tools, and migrate LDAP user entitlements from the data-va Virtual Machine to the service-va Virtual Machine.

Migrate LDAP User Entitlements from the data-va Virtual Machine to the service-va Virtual Machine

4

For Horizon Workspace 1.8, LDAP user entitlements move from the data-va virtual machine to the service-va virtual machine. Horizon Workspace 1.8 requires that you migrate LDAP user entitlements to the service-va virtual machine to successfully complete the upgrade.

The time it takes to migrate LDAP user entitlements from the data-va virtual machine to the service-va virtual machine is based on the number of entitled users in your environment. It takes approximately one hour per 10,000 users to migrate LDAP user entitlements. The script deletes user entries from the data-va virtual machine's LDAP server during the migration process.

If the migration process is interrupted while it is in progress, when you run it again, the process resumes from where it stopped. During the migration, all Horizon Workspace services are stopped, so plan the upgrade with the expected downtime in mind.

NOTE If you experience a problem during the migration process, refer to the log file which is located at `/opt/zimbra/alwaysOnMigration.log`.

Prerequisites

- Update all virtual machines on all nodes with the latest version of Horizon Workspace 1.8.
- Take a snapshot of the vApp to back it up. For information about how to take a snapshot, see vSphere documentation.
- Turn on maintenance mode for all the data-va virtual machines.

  NOTE To turn on maintenance mode for a virtual machine, open the configurator-va virtual machine and click the **Enter Maintenance Mode** link to turn off each virtual machine.
- Turn on maintenance mode for all service-va virtual machines except the main service-va virtual machine.
- From the Directory Sync page on the connector-va virtual machine, change the scheduling frequency to `Manual`. See *Installing and Configuring Horizon Workspace Guide* for information about enabling Directory Sync on the connector.

IMPORTANT After you turn maintenance mode on, you must wait at least two minutes for the changes to occur on the gateway-va virtual machines.

Procedure

1 Use ssh to connect to the master data-va virtual machine running OpenLDAP.

2 Change to the Zimbra user.

```
su – zimbra
```

3 Run the LDAP migration script.

```
alwayson-ldap-migration
```

4 (Optional) If the LDAP migration script (`alwayson-ldap-migration`) fails to run, run the script again with verbose mode to show progression messages during the migration.

```
alwayson-ldap-migration -v
```

5 Turn maintenance mode off for the service-va virtual machines and data-va virtual machines.

NOTE To turn maintenance mode off for a virtual machine, open the configurator-va virtual machine and click the **Exit Maintenance Mode** link to turn each virtual machine back on.

What to do next

Continue post-upgrade configuration tasks.

Configuring Horizon Workspace 1.8 after an Upgrade 5

After you complete the upgrade to Horizon Workspace 1.8, you can perform configuration tasks, such as adding or resizing a buffer disk, updating configuration settings for connector-va virtual machines, configuring SSO for Desktop clients, and so on.

This chapter includes the following topics:

Add or Resize a Disk for Buffering Files

The gateway-va virtual machine buffers client requests before sending them to the data-va virtual machine. Large files that are waiting to upload are temporarily stored on this disk. Depending on the upload size limit set for your environment, the space on the buffer disk can easily exceed the maximum limit.

During the Horizon Workspace 1.8 installation, an additional disk is created and configured for the gateway-va virtual machine to use to buffer files waiting to upload.

The Horizon Workspace 1.8 upgrade creates the configuration that points to an additional buffer disk on the gateway-va virtual machine. However, you can create the buffer disk only after the upgrade is complete.

Procedure

1 Stop the gateway-va virtual machine.

```
/etc/rc.d/nginx stop
```

2 (Optional) To increase or decrease the disk size allotted to the buffer, delete the disk.

3 Create a new disk.

4 Remove the existing sub-directories: `proxy_temp` and `client_body_temp`.

5 Mount the disk at `/opt/vmware/nginx/buffer`.

6 Start the gateway-va virtual machine.

```
/etc/rc.d/nginx start
```

What to do next

When the gateway-va virtual machine buffers large files, the end user's performance is not usually affected. If large files do affect performance, increase the disk space allotted to the buffer.

Updating the Connector Configuration Settings

Horizon Workspace authenticates users based on several configurations, including authentication methods, default access policy set, network ranges, and identity provider instances.

See the *Horizon Workspace Administrator's Guide* for a detailed description of user stores, authentication scores, network ranges, and default access policy set.

Update the User Store Configuration Settings

Horizon Workspace creates a default user store for you during the upgrade process. Each user store has a sync client that you select for syncing users and groups to Horizon Workspace. After an upgrade, you must update the sync client and verify the user authentication identity provider.

If necessary, you can edit the user store settings to allow users to log in with a domain name. If you want to add a user store, see the *Horizon Workspace Administrator's Guide*.

Procedure

1 Log in to the Administrator Web interface.

2 Select **Settings > User Stores**.

3 Click **Edit** for the user store you want to configure.

4 Edit the user store settings.

Option	Description
Sync Client	After upgrading from Horizon Workspace 1.5 to Horizon Workspace 1.8, you must update the sync client by selecting a Connector instance so that users and groups can be synced to the user store. NOTE If you do not update the sync client after an upgrade, the next directory sync fails.
Verify the User Authentication Identity Provider	During the upgrade, the user authentication identity provider is selected. Verify that the correct identity provider was selected. If you want to use a different identity provider, you can select a different one.
(Optional) Display user store name instead of domain name for end user authentication	Click the check box for this option to allow users to log in with the user store name, as it appears in the Name text box, instead of with domain names. If you do not select the check box, users are presented with the domain names listed in the User Domains section.

5 Click **Save**.

What to do next

If you have not already done so, associate the user store with an identity provider instance.

Update Identity Provider Settings

After you upgrade from Horizon Workspace 1.5 to Horizon Workspace 1.8, you must set or verify the identity provider configuration settings.

Procedure

1 Log in to the Administrator Web interface.

2 Select **Settings > Identity Providers**.

3 Edit the identity provider instance settings.

Option	Description
User Store	Verify that the user store selected during the upgrade is the one you want to use in your environment. Select all the user stores you want to associate with this identity provider instance.
Authentication Method	Verify that the authentication methods selected during the upgrade are appropriate for your environment. Select the authentication methods for Horizon Workspace to apply when users who are associated with this identity provider instance log in. **NOTE** See the *Installing and Configuring Horizon Workspace Guide* for information about authentication.
Network Ranges	Verify that the network ranges selected are appropriate for your environment. The network ranges text box lists the existing network ranges in your Horizon Workspace deployment. Select the network ranges of the users, based on their IP addresses, that you want to direct to this identity provider instance for authentication.

4 Click **Save**.

What to do next

After an upgrade, you must configure new policies if you do not want to use the default policy set.

Configure the Default Policy

During the Horizon Workspace upgrade process, the default policy is automatically set. If you use different policies in your environment, you must set up your policies. You must add a policy for each network range, and select the desired authentication method and authentication score.

Horizon Workspace includes a default access policy set that controls user access to Horizon Workspace User Portal. You can edit the policy set by editing, deleting, or adding policies as necessary.

Each policy in the default access policy set requires that a set of criteria be met in order for Horizon Workspace to allow access to the user portal.

You can edit the default access policy set, which is a pre-existing policy set that controls user access to Horizon Workspace as a whole. The default access policy set is permanent. You can edit it, but you cannot remove it. You can edit the default access policy set by removing existing policies from the set, editing existing policies in the set, or adding new policies to the set.

Procedure

1 Log in to the Administrator Web interface.

2 Select **Policies > Access Policy Sets**.

3 Click **Edit** to configure the existing policy set.

4 If necessary, change the policy set name and description in the respective text boxes.

NOTE Horizon Workspace displays the text in the Policy Set Name and Description text boxes in English. You can edit this text, which includes changing the text to a different language.

5 Configure the policy set to suit your environment.

a Click the policy name to edit or remove a policy.

b (Optional) If you want to add a new policy, click the **+ Access Policy** button.

c Select the correct network ranges from the Network drop-down menu.

d Select the correct Authentication Score from the Minimum Authentication Score drop-down menu.

e Verify that the TTL value meets the requirement for access to Horizon Workspace.

6 Click **Save**.

What to do next

The default policy is applied to all the applications in the catalog. If you want to write specific application access policies, see the *Horizon Workspace Administrator's Guide*.

Configure SSO for Desktop Clients

To configure Horizon Workspace to use single sign-on by default from the Desktop clients, you must add a new parameter to the `runtime-config.properties` file on the service-va virtual machine. Otherwise, end users must log in to access the user portal first.

Procedure

1 Log in to the service-va virtual machine as administrator.

2 Open the `runtime-config.properties` file.

```
/usr/local/horizon/conf/runtime-config.properties
```

3 Add the `apply.login.ota=true` parameter to the `runtime-config.properties` file.

4 Run the `restart` command to restart the service-va virtual machine.

```
/etc/init.d/horizon-frontend restart
```

End users can use single sign-on to log in to Horizon Workspace.

Configure Your Horizon Workspace System to Update Resources Used By VMware Ready Android Devices

If your organization plans to use the capabilities that Horizon Workspace provides for VMware Ready Android devices, you must perform some additional configuration steps after upgrading your Horizon Workspace 1.5 deployment to Horizon Workspace 1.8.

Because the upgrade process leaves intact the existing configuration of the resources used by VMware Ready Android devices, you must update the configuration related to these resources.

After you upgrade the Horizon Workspace vApp, a newer version of the Android workspace image, the secure workspace container, is available in the filesystem of the service-va, and newer versions of the default Android mobile applications are available in your catalog. By default, these newer versions do not overwrite the versions that existed in your catalog prior to upgrading your server. User and group entitlements to the previous version of the Android workspace image and uploaded Android applications that were configured in your Horizon Workspace system prior to the upgrade remain configured. Users and groups are not automatically entitled to the newer versions of the Android workspace image or the default Android mobile applications.

The resources you must update include:

- The Android workspace image which provides the secure container for the managed mobile workspace. You must obtain the newer Android workspace image from the service-va, upload it into your catalog, and entitle those users and groups that are currently entitled to the older Android workspace image to the newer one.

- Entitlements to the Horizon Workspace for Android app. The Horizon Files for Android app is the newer version of the Horizon Workspace for Android app. This mobile application is used to provide the file-sharing capabilities in the managed mobile workspaces on VMware Ready Android devices. After the upgrade process, the newer Horizon Workspace for Android app is provided in your catalog by default. You must entitle those users and groups that are currently entitled to the Horizon Workspace for Android app to the Horizon Files for Android app, and then unentitle them from the Horizon Workspace for Android app.
- Entitlements to other Android apps that have newer versions in your catalog after the upgrade process. You must entitle those users and groups that are currently entitled to an older app to the newer version of the app.

Prerequisites

- Verify that your Horizon Workspace deployment has the 1.8 version level.
- Verify that you can use ssh and the sshuser account to log in to the service-va. You must be able to download a file from the service-va's filesystem using ssh.

  For the steps on how to connect to the service-va using ssh, see the VMware knowledge base article at http://kb.vmware.com/kb/2061672.

  To set a password for the sshuser account on the service-va, log in to the service-va as the root user using the vSphere client console and the service-va's command-line interface console. Run the command `passwd sshuser` to set the password.

Procedure

1 Obtain the ZIP file for the Android workspace image from the filesystem of the service-va.

   a Launch an SSH client session and connect to the service-va.

   b Log in as the sshuser.

   c Copy the file `/opt/vmware/mobile/vvp.zip` to a local system so that it is available for uploading into your catalog using the Administrator Web interface.

2 Upload the Android workspace image into your catalog.

   a Log in to the Administrator Web interface.

   b Click the **Catalog** tab.

   c Select **+ Add Application > Android Workspace Image ... from a zip file**.

   d Select the vvp.zip file that you downloaded and click **Upload**.

   The new version, v4.2.2, of the Android workspace image is displayed on your Catalog page and now available for entitling to users and groups.

3 Obtain the list of groups and users that are currently entitled to the Horizon Workspace 1.5 release's Android workspace image, the v2.3.6 version.

   To update these groups and users to the 1.8 version of the Android workspace image, you must entitle them to the newer one. Using the resource' page from the Catalog page is the fastest way to see the entire list of currently entitled users and groups.

   a Click the **Catalog** tab.

   b Restrict the view to only list the Android workspace images that are in your catalog by selecting **Any Application Type > Android Workspace Images**.

   c Click the entry that is has a name containing VMware Android v2.3.6.

   The entry's resources page is displayed, usually with the Entitlements page selected by default.

   d. If the Entitlements page is not displayed, select **Entitlements** to see the currently entitled groups and users.

   e. Make note of the names of groups in the Group Entitlements table and the names of users in the Individual Entitlements table.

4. Entitle the groups and users to the new Android workspace image.

   a. Click the **Catalog** tab.

   b. Restrict the view to only list the Android workspace images that are in your catalog by selecting **Any Application Type > Android Workspace Images**.

   c. Click the entry that is has a name containing VMware Android v4.2.2.

      The application's resources page is displayed, usually with the Entitlements page selected by default.

   d. If the Entitlements page is not displayed, select **Entitlements**.

   e. Add the group entitlements and user entitlements to match the ones you noted from the Entitlements page for the VMware Android v2.3.6 entry.

   f. Click **Done** to apply your changes.

   The next time a currently provisioned device syncs with this Horizon Workspace system, a notification displays on the device to notify the user that you have updated the secure workspace container and Switch will clear and reboot their workspace to apply the update. By default, data that is locally stored in the managed workspace on the device is deleted as part of applying the update.

5. Obtain the list of groups and users that are currently entitled to the Horizon Workspace 1.5 release's Horizon Workspace for Android mobile application.

   a. Click the **Catalog** tab.

   b. Restrict the view to only list the Android mobile applications that are in your catalog by selecting **Any Application Type > Mobile Applications**.

   c. Click the application that is labeled Workspace.

      The application's resources page is displayed, usually with the Entitlements page selected by default.

   d. If the Entitlements page is not displayed, select **Entitlements** to see the currently entitled groups and users.

   e. Make note of the names of groups in the Group Entitlements table and the names of users in the Individual Entitlements table.

      To update those groups and users to the 1.8 version of the mobile application, you must entitle them to the Horizon Files for Android mobile application, and then remove their entitlements from the Horizon Workspace for Android mobile application.

6. Entitle the groups and users to the new Horizon Files for Android mobile application.

   a. Click the **Catalog** tab.

   b. Restrict the view to only list the Android mobile applications that are in your catalog by selecting **Any Application Type > Mobile Applications**.

   c. Click the application that is labeled VMware Horizon Files.

      This mobile application is the Horizon Files for Android application for use with Horizon Workspace 1.8 systems.

      The application's resources page is displayed, usually with the Entitlements page selected by default.

d If the Entitlements page is not displayed, select **Entitlements**.

e Add the group entitlements and user entitlements to match the ones you noted from the Horizon Workspace for Android application's Entitlements page.

f Click **Done** to apply your changes.

7 Remove the entitlements from the older Horizon Workspace for Android application.

a Click the **Catalog** tab.

b Restrict the view to only list the Android mobile applications that are in your catalog by selecting **Any Application Type > Mobile Applications**.

c Click the application that is labeled Workspace.

The application's resources page is displayed, usually with the Entitlements page selected by default.

d If the Entitlements page is not displayed, select **Entitlements** to see the currently entitled groups and users.

e Remove the group and user entitlements, and click **Done** to apply your changes.

8 Verify the user and group entitlements for the remaining Android apps that are provided by the upgrade process by default, and entitle the users and groups to the newer versions, as appropriate for your organization's needs.

Such Android apps appear in your catalog twice with the same name, like the OfficeSuite app and the Socialcast app.

NOTE You do not have to configure the entitlements for the newer VMware Horizon Mail app, because its entitlements are automatically configured with entitlements to the Android workspace image.

The groups and users that had been entitled to the older Android workspace image are now entitled to the appropriate newer Android workspace image for use with your Horizon Workspace 1.8 system. The groups and users that had been entitled to the Horizon Workspace for Android mobile application that was used for Horizon Workspace 1.5 systems are now entitled to the appropriate Horizon Files for Android application for use with your Horizon Workspace 1.8 system. The managed mobile workspaces on the VMware Ready Android devices that are managed by this Horizon Workspace system are updated with the new secure workspace container and the newer applications the next time the devices sync with your Horizon Workspace system. For a description of the syncing and leasing process for VMware Ready Android devices, see the *Horizon Workspace Administrator's Guide*.

What to do next

You must remove the older versions of the Android workspace image, VMware Email app, and the other Android mobile apps from your catalog. Removing the older versions from the your catalog prevents the risk of entitling groups and users to the older versions, and ensures they receive the advantages of the improvements provided in the new versions.

To remove the older versions of the Android workspace image and VMware Email app, you must first enable their deletion by completing the steps in "Enable Deletion of Prior Versions of the Android Workspace Image and VMware Email Mobile App Resources," on page 24. Then you can remove the older versions of the resources by using the Delete button on their individual resource pages in the Administrator Web interface.

Enable Deletion of Prior Versions of the Android Workspace Image and VMware Email Mobile App Resources

By default, the Administrator Web interface does not provide a **Delete** button on the resources pages for the Android workspace image and the VMware Email mobile app. So that you can delete the older versions of those resources from your catalog after you have entitled your groups and users to the newer versions, you must configure your Horizon Workspace system to enable the display of the Delete button on the resource pages for those resources.

After you upgrade your Horizon Workspace system and update your group and user entitlements to the new version of the Android workspace image and VMware Horizon Mail app used on VMware Ready Android devices, you must remove the older versions of those resources from your catalog. Removing the older versions from the your catalog prevents the risk of entitling groups and users to the older versions, and ensures they receive the advantages of the improvements provided in the new versions.

Because the **Delete** button is not displayed by default in the Administration Web interface for those older resources, the Android workspace image and the VMware Email app, you must first configure your Horizon Workspace system to enable display of the **Delete** button so that you can use it to remove the older versions of those resources.

IMPORTANT Some of the steps in this procedure involve modifying the data in one of the database tables in the database that is configured for your Horizon Workspace deployment. Use the those methods and database administration tools for working with database tables that are standard and appropriate for the type of database that is configured for your deployment. For production environments, the database server is typically an external Oracle or vFabric Postgres database server, and you use the methods and database administration tools that your organization typically uses with that database server. If you are making these changes in a proof-of-concept deployment that uses the internal database, you must first configure the service-va virtual machine to enable remote access to the internal database so that you can use a database administration tool to access the internal database running in the service-va.

Prerequisites

- Complete the steps in "Configure Your Horizon Workspace System to Update Resources Used By VMware Ready Android Devices," on page 20.
- Verify that you have the appropriate database administration client tool and access information for making changes to database tables in the external database server that is configured for your Horizon Workspace deployment.
- If your Horizon Workspace deployment is configured to use the internal database and you do not have an existing database administration client tool for working with the database, download and install the pgAdmin tool from www.pgadmin.org. The pgAdmin tool is an administration tool used with Postgres open-source databases.
- If your Horizon Workspace deployment is configured to use the internal database, verify that you can log in to the service-va's command-line interface either using the service-va's console in the vSphere Client and the root user and the root user's password or using ssh and the sshuser account and the sshuser account's password. You must be able to perform command-line operations in the service-va's filesystem.

  For the steps on how to connect to the service-va using ssh, see the VMware knowledge base article at http://kb.vmware.com/kb/2061672.

  To set a password for the sshuser account on the service-va if the password has not been previously set, log in to the service-va as the root user using the vSphere client and the service-va's console. Run the command `passwd sshuser` to set the password.

Procedure

1 If your deployment is using the internal database, you must configure the internal database in your service-va virtual machine to accept external requests from pgAdmin or other type of database administration tool.

   a Log in to the service-va virtual machine's command-line interface using the vSphere Client and the `root` user account and password.

   b Edit the database client configuration file, `/db/data/pg_hba.conf` to add a line as the last line of the file.

   ```
   host   all    all   0.0.0.0/0   md5
   ```

   NOTE This line must be the last line of text in the `pg_hba.conf` file. This line might already exist as the last line of text in the file.

   c Save the file.

   d Edit database configuration file, `/db/data/postgresql.conf`, to change the `listen_addresses = 'localhost'` line to `listen_addresses = '*'`.

   ```
   listen_addresses = '*'
   ```

   e Save the file.

   f Restart the vpostgres service.

   ```
   service vpostgres restart
   ```

   Wait for the message that states the service is back online.

   g Run the `iptables` command to open incoming TCP port 5432.

   ```
   iptables -A INPUT -p tcp --dport 5432 -j ACCEPT
   ```

   Port 5432 is the standard TCP port used for the `vpostgres` service. Running this command opens port 5432 so that your database administration tool can communicate with internal database system. This change is reverted the next time you stop and restart the service-va virtual machine, or when you add virtual machines to the Horizon Workspace vApp.

   h Verify the change is in effect by listing the local iptable rules.

   ```
   iptables -nL -v --line-numbers | grep -i 5432
   ```

   The output should be similar to the following line.

   ```
   25 0 0 ACCEPT tcp -- * * 0.0.0.0/0 0.0.0.0/0 tcp dpt:5432
   ```

   i Verify the `vpostgres` service is up and running.

   ```
   service vpostgres status
   ```

2 Use your database administration tool to access the Resource database table in the database used for your Horizon Workspace deployment.

3 Locate the table row that corresponds to the catalog resource entry for the older VMware Email app.

   The Resource database table has column named resourceName, and that column contains the value `VMware Mail` in the row that corresponds to the older VMware Email app.

4 For that table row, modify the value in the definition column to update the portion `"isMandatory":true` to `"isMandatory":false`.

5 Locate the table row that corresponds to the catalog resource entry for the older Android workspace image.

   Look for a row where the value in the resourceName column contains `VMware Android v2.3.6`.

6 For that table row, modify the value in the definition column to update the portion `"isMandatory":true` to `"isMandatory":false`.

7 Save your changes.

8 Stop and restart your service-va virtual machine using the vSphere Client.

Restarting the service-va virtual machine closes port 5432.

In the Administrator Web interface, the resources pages for the VMware Email app and VMware Android v2.3.6 workspace image each display a **Delete** button. You are able to use that button to remove those previous versions from your catalog.

What to do next

Remove the older versions of the Android workspace image and the VMware Email app by logging into the Administrator Web interface, opening their resource pages from the Catalog page, and clicking the **Delete** button.

Updating VMware Tools for Horizon Workspace Virtual Machines

6

You can update VMware® Tools™ in the vSphere® client in Horizon Workspace 1.8. Each time you power on a virtual machine the guest operating system checks the version of VMware Tools. The status bar of the virtual machine displays a message when a new version is available.

See the vSphere Documentation Center for information about updating VMware Tools.

Troubleshooting Installation Errors 7

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

This chapter includes the following topics:

Using the Error Logs

Resolve errors that occurr during your Horizon Workspace upgrade from version 1.5 to version 1.8 by reviewing the error logs.

Problem

After the upgrade finishes, Horizon Workspace version 1.8 does not open and errors occur.

Cause

The errors must be resolved to proceed with the installation.

Solution

1. Go to the directory located at `/opt/vmware/var/log`.
2. Open the `update.log` file and review the error messages.
3. Resolve the errors and rerun the upgrade command again to successfully upgrade to Horizon Workspace 1.8. When you rerun the upgrade command, it resumes from the point where it stopped.

NOTE Alternatively, you can revert to a snapshot and run the update again.

Rolling Back to Snapshots of Horizon Workspace

If Horizon Workspace does not start properly after an upgrade, roll back to a previous instance.

Problem

After you run the `updatemgr.hzn` command, Horizon Workspace does not start correctly.

Cause

Errors occurred during the upgrade process. To review error messages in the error log and resolve them, see "Using the Error Logs," on page 29.

Solution

- ◆ To revert to one of the snapshots you took as a backup of your original Horizon Workspace instance and external database, if applicable, see the vSphere documentation.

Saving the ThinApp Package Configuration or Syncing ThinApp Packages Fails After Upgrade

When you make a change in the ThinApp packages configuration in the Connector Web interface and try to save your changes, or when you try to manually sync ThinApp packages using the Connector Web interface, an error occurs.

Problem

After upgrading your Horizon Workspace server, when you click the **Save** button or the **Sync Now** button for the ThinApp packages' configuration in the Connector Web interface, the save or sync operation fails and an error message appears. The error messages that might appear include:

- `Error configuring packaged applications: RepoUpdateRegistry() failed with error: LW_ERROR_PASSWORD_MISMATCH: The password is incorrect for the given username.`
- `Error occurred in Packaged applications (ThinApp) sync. Please check if Packaged applications (ThinApp) configuration is correct and the share path is reachable.`

Cause

After an upgrade, the Connector can be in a state where it is not joined to the Active Directory domain, even though the Connector Web interface indicates the Connector is joined to the domain.

Solution

1. Log in to the Connector Web interface.
2. Click **Join Domain**.
3. Click **Leave Domain**, and responding **Yes** to confirm.
4. Rejoin the domain by selecting the **Join Domain** check box and entering the appropriate Active Directory domain, user name, and password for your deployment.
5. Click **Packaged Apps - ThinApps** and re-try saving the ThinApp configuration or syncing the ThinApp packages.

Index