Horizon Cloud with Hosted Infrastructure Administration

VMware Horizon Cloud Service
Horizon Cloud with Hosted Infrastructure 17.2
You can find the most up-to-date technical documentation on the VMware website at:
https://docs.vmware.com/
If you have comments about this documentation, submit your feedback to
docfeedback@vmware.com
Contents

1 About Horizon Cloud with Hosted Infrastructure Administration 6

2 The Horizon Cloud Administration Console 7
   Using the Console's Search Feature 7
   Using the Filter Field in the Administration Console 8
   The User Card in the Horizon Cloud Administration Console 9
   Terms Used in the Administration Console 10

3 Getting Started Wizard 11

4 Join or Leave the Customer Experience Improvement Program 14

5 Monitoring 15
   Dashboard Page 15
   Activity Page 16
   Reports Page 17
   Notifications Page 18

6 Assignments 20
   Types of Assignments 21
   Capacity and Users Values for VDI Desktop Assignments 23
   Create an Application Assignment 23
   Create a Dedicated or Floating VDI Desktop Assignment 24
   Create an RDSH Session Desktop Assignment 26
   Edit an Assignment 28
   Create a URL Redirection Configuration 29
   Edit Assignment Mode 36
   Update Agents for an Assignment 37
   Delete an Assignment 38
   Recover an Assignment 39
   Manage Desktops in a Dedicated or Floating Desktop Assignment 39
   View System or User Activity for Assignments 40
   Working with Nested Organizational Units 41

7 Applications 42
   Importing New Applications from an RDSH Farm Using Auto-Scan from Farm 43
   Manually Adding Custom Applications from an RDSH Farm 44
   Edit an Application 45
15  Technical Notes  138

16  Helpdesk Console (Beta Feature)  139
   Access the Helpdesk Console  139
   Launch a Console for a Virtual Machine  140
   Set Up a Health Scan  140
   Get Remote Assistance  142
   View Usage Report  142
   Image Upload  142
   View History  147
About Horizon Cloud with Hosted Infrastructure Administration

This guide provides information on how to create, deploy, and administer virtual desktops and applications using Horizon Cloud.

Intended Audience

This document is intended for experienced IT system administrators who are familiar with virtual machine technology and datacenter operations.

VMware Technical Publications Glossary

VMware Technical Publications provides a glossary of terms that might be unfamiliar to you. For definitions of terms as they are used in VMware technical documentation, go to http://www.vmware.com/support/pubs.
The Horizon Cloud Administration Console

The Horizon Cloud Administration Console is the tenant administration interface for Horizon Cloud. The topics in this section provide general information about the Administration Console.

This chapter includes the following topics:
- Using the Console’s Search Feature
- Using the Filter Field in the Administration Console
- The User Card in the Horizon Cloud Administration Console
- Terms Used in the Administration Console

Using the Console’s Search Feature

Use the Horizon Cloud Administration Console’s search feature to locate a specific user or virtual machine (VM) by name in your environment.

You open the search box by clicking the magnifying glass icon ( ) in the header portion of the Administration Console. Then you can select to search within either users or VMs. When you have typed at least three (3) characters in the search field, names that begin with those characters are displayed. You can continue typing in more characters to narrow down the results.
Note  With the VMs search, you can search for RDS server VMs in farms and VDI desktop VMs.

When you see the one you are searching for, you can click it to get more details about the user or VM. The screen that is displayed depends on whether you clicked on a user or a VM:

- For a user, the card for that user is displayed. For details, see The User Card in the Horizon Cloud Administration Console.
- For a VM, the system displays the screen on which you can locate that VM. For example, if you click on a VM in the results list that is an RDS server VM in a farm, the system displays the Servers tab of that farm's details page.

Using the Filter Field in the Administration Console

Various pages in the Horizon Cloud Administration Console provide a filter field to filter the information that is displayed on those pages.

When a page has a filter field, as you type characters into the field, the system displays only the subset of records that contain characters that match that pattern.

Note  The system begins matching the pattern and filtering the records displayed in the page after you have typed three (3) characters into the filter field.
The User Card in the Horizon Cloud Administration Console

Use the Horizon Cloud Administration Console's user card feature as a dashboard to work with a specific user's assigned resources, such as that user's assignments.

You use the Administration Console's search feature to display the card for a specific user. See Using the Console's Search Feature for how to search for a user. When you click on a user in the search results, that user's card is displayed.

Use the tabs at the top of the user card to work with those items in your environment that are related to that user.

<table>
<thead>
<tr>
<th>User Card Tabs</th>
<th>Description</th>
</tr>
</thead>
</table>
| Assignments    | Lists the user's assignments.  
| Note           | When a user is entitled to a dedicated VDI desktop assignment, but has not yet launched the desktop for the first time, that assignment appears on the Assignments tab. However, after the user's first launch of the desktop, the system removes it from the Assignments tab's list and displays it on the Desktops tab. |
| Desktops       | Lists the user's active desktop sessions.  
| Note           | For a VDI dedicated desktop assignment, when the user launches the entitled VDI dedicated desktop for the first time, the system permanently assigns that VDI dedicated desktop to that user. As a result, the Desktops tab always lists the user's entitled VDI dedicated desktops after their initial use, even if the user does not have an active session to those desktops |
| Applications   | Lists the user's entitled native and remote applications. |
User Card Tabs | Description
--- | ---
Writable Vol | Lists the user's entitled writable volumes.
Activity | Displays the user's activity for selected time periods.

Terms Used in the Administration Console

The Horizon Cloud Administration Console replaced the Enterprise Center, and some of the terms used in the interface are different.

The table below shows common Enterprise Center terms and their equivalents in the Horizon Cloud Administration Console.

<table>
<thead>
<tr>
<th>Enterprise Center</th>
<th>Horizon Cloud Administration Console</th>
</tr>
</thead>
<tbody>
<tr>
<td>Desktop Manager</td>
<td>Pod</td>
</tr>
<tr>
<td>User Activity</td>
<td>Activity</td>
</tr>
<tr>
<td>Task and Events</td>
<td>Activity</td>
</tr>
<tr>
<td>Pool</td>
<td>Assignment</td>
</tr>
<tr>
<td>Session-based Pool (Desktop-only)</td>
<td>Session Desktop Assignment</td>
</tr>
<tr>
<td>Session-based Pool (Application-only)</td>
<td>Remote Application Assignment</td>
</tr>
<tr>
<td>Static Pool</td>
<td>Dedicated Desktop Assignment</td>
</tr>
<tr>
<td>Dynamic Pool</td>
<td>Floating Desktop Assignment</td>
</tr>
<tr>
<td>Mapped</td>
<td>Assigned User</td>
</tr>
<tr>
<td>Dynamic Pool Refresh</td>
<td>Push Updates</td>
</tr>
<tr>
<td>Gold Pattern</td>
<td>Image</td>
</tr>
<tr>
<td>Sealed Gold Pattern</td>
<td>Published Image</td>
</tr>
<tr>
<td>Unsealed Gold Pattern</td>
<td>Offline Image</td>
</tr>
</tbody>
</table>
Getting Started Wizard

The Getting Started wizard displays by default when you open the user interface, showing the tasks necessary to set up your Horizon Cloud system. The wizard provides a high-level overview of the work that you have done, and what you still need to do. You can access this page at any time by clicking the 'play' icon at the top of the page.

It is recommended that you perform the tasks in the order shown.

**Note** When you log in for the first time, you must register the Active Directory before you can start using the system. See below under General Setup.
<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>General Setup</td>
<td>Includes tasks related to general settings.</td>
</tr>
<tr>
<td></td>
<td>- Active Directory</td>
</tr>
<tr>
<td></td>
<td>- To add first AD domain:</td>
</tr>
<tr>
<td></td>
<td>a Click the <strong>Add</strong> button under Active Directory.</td>
</tr>
<tr>
<td></td>
<td>b Follow steps in Register Your First Active Directory Domain.</td>
</tr>
<tr>
<td></td>
<td>- To edit the AD domain:</td>
</tr>
<tr>
<td></td>
<td>a Click the <strong>Edit</strong> button under Active Directory.</td>
</tr>
<tr>
<td></td>
<td>b Follow steps in Edit an Active Directory Domain.</td>
</tr>
<tr>
<td></td>
<td>- Roles and Permissions</td>
</tr>
<tr>
<td></td>
<td>- To edit roles and permissions:</td>
</tr>
<tr>
<td></td>
<td>a Click the <strong>Edit</strong> button under Roles &amp; Permissions.</td>
</tr>
<tr>
<td></td>
<td>b Follow the steps in Edit Roles and Permissions.</td>
</tr>
<tr>
<td></td>
<td>- User Session Information</td>
</tr>
<tr>
<td></td>
<td>This feature allows user and domain data to be used by the Cloud Monitoring</td>
</tr>
<tr>
<td></td>
<td>Service (CMS) for reports on the Reports page. If it is disabled, the</td>
</tr>
<tr>
<td></td>
<td>following are not provided:</td>
</tr>
<tr>
<td></td>
<td>- The Unique User Summary feature of the Utilization report</td>
</tr>
<tr>
<td></td>
<td>- The Session History report</td>
</tr>
<tr>
<td></td>
<td>a Click the <strong>Edit</strong> button under User Session Information.</td>
</tr>
<tr>
<td></td>
<td>b To keep the feature enabled, leave the default setting (YES) and click</td>
</tr>
<tr>
<td></td>
<td><strong>Save</strong>. To disable, switch the setting to NO and click <strong>Save</strong>.</td>
</tr>
<tr>
<td></td>
<td>You can return to this setting and change it at any time, either in the</td>
</tr>
<tr>
<td></td>
<td>Getting Started wizard or in General Settings.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> The agents on the virtual machines (RDSH and VDI) need outbound</td>
</tr>
<tr>
<td></td>
<td>Internet access so they can send the data to Horizon Cloud.</td>
</tr>
<tr>
<td>Desktop Assignment</td>
<td>Includes tasks related to creating desktop assignments.</td>
</tr>
<tr>
<td></td>
<td>- To create an image:</td>
</tr>
<tr>
<td></td>
<td>a Click the <strong>New</strong> button under Create Image.</td>
</tr>
<tr>
<td></td>
<td>b Follow the steps in Create an Image.</td>
</tr>
<tr>
<td></td>
<td>- To create a desktop assignment:</td>
</tr>
<tr>
<td></td>
<td>a Click the <strong>New</strong> button under Create New Desktop Assignment.</td>
</tr>
<tr>
<td></td>
<td>b Follow the steps in Create a Dedicated or Floating VDI Desktop</td>
</tr>
<tr>
<td></td>
<td>Assignment or Create an RDSH Session Desktop Assignment, depending on</td>
</tr>
<tr>
<td></td>
<td>the type of desktop assignment you want to create. For more information,</td>
</tr>
<tr>
<td></td>
<td>see Types of Assignments.</td>
</tr>
<tr>
<td>Application Assignment</td>
<td>Includes tasks related to creating application assignments.</td>
</tr>
<tr>
<td></td>
<td>- To create an RDSH image:</td>
</tr>
<tr>
<td></td>
<td>a Click the <strong>Configure</strong> button under Create RDSH Image.</td>
</tr>
<tr>
<td></td>
<td>b Follow the steps in Create an RDSH Image.</td>
</tr>
<tr>
<td></td>
<td>- To create an application farm:</td>
</tr>
<tr>
<td></td>
<td>a Click the <strong>New</strong> button under Create Application Farm.</td>
</tr>
<tr>
<td></td>
<td>b Follow the steps in Create a Farm.</td>
</tr>
<tr>
<td></td>
<td>- To review application inventory:</td>
</tr>
<tr>
<td></td>
<td>a Click the <strong>Go</strong> button under Application Inventory.</td>
</tr>
<tr>
<td>Section</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td></td>
<td>Review and edit applications on the Applications page as described in Chapter 7 Applications.</td>
</tr>
<tr>
<td></td>
<td>To create a new application assignment:</td>
</tr>
<tr>
<td></td>
<td>Click the New button under Create New Application Assignment.</td>
</tr>
<tr>
<td></td>
<td>Follow the steps in Create an Application Assignment.</td>
</tr>
</tbody>
</table>

At the bottom of the page, use the slider to indicate if you want the Getting Started page to appear at startup.
Join or Leave the Customer Experience Improvement Program

The VMware Customer Experience Improvement Program (CEIP) provides information that VMware uses to improve its products and services, to fix problems, and to advise you on how best to deploy and use VMware products.

Horizon Cloud participates in the VMware CEIP. Information about the data collected through CEIP and how VMware uses it are in the Trust & Assurance Center at http://www.vmware.com/trustvmware/ceip.html.

The CEIP appears the first time you start Horizon Cloud after completing the domain join. You must then make a selection. You can change your selection at any time after that.

Procedure

1. Start the Horizon Cloud Administration Console.

2. Select Help > CEIP.

3. Move the slider next to Join Customer Experience Improvement Program to No to leave CEIP or Yes to join. The default is Yes.

4. Click Save.
Monitoring

Use the Monitor icon to access desktop information, administrator and user activity, view reports detailing user and desktop mapping, and check notifications.

There are four selections available from the Monitor icon.

<table>
<thead>
<tr>
<th>Selection</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dashboard</td>
<td>Displays details on desktop connections, connection states, and capacity allocation.</td>
</tr>
<tr>
<td>Activity</td>
<td>Displays activity details for Administrators and Users.</td>
</tr>
<tr>
<td>Reports</td>
<td>Provides mapping details for Users and Desktops</td>
</tr>
<tr>
<td>Notifications</td>
<td>Displays a list of current notifications.</td>
</tr>
</tbody>
</table>

This chapter includes the following topics:

- Dashboard Page
- Activity Page
- Reports Page
- Notifications Page

Dashboard Page

This page is available from the Monitor icon and displays information about your overall environment.

The system refreshes the information every few minutes and displays a message indicating the amount of time remaining until the next refresh. You can also refresh the page manually.
### Activity Page

The Activity page shows data regarding current and past events in the system.

The Activity page is available from the Monitor icon. You can perform these tasks.

- Use the Show filter to display events for only a certain period of time.
- View the total number of events.
- Use the Filter box to filter events.
- Refresh the list.
- Download information in the list in .xlsx format with the Export feature.

The Activity page contains tabs for administrator and user events.

### Administrator Events

The Administrator tab displays administrator events with information for each action. Expand an event to view details and subtasks for that event.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Details regarding the event.</td>
</tr>
<tr>
<td>Percentage Completion</td>
<td>Current percentage of event completed.</td>
</tr>
<tr>
<td>Status</td>
<td>Successful indicates an event was performed in its entirety. Failed indicates an event was either partially performed or not performed at all.</td>
</tr>
<tr>
<td>Time</td>
<td>Time that the event was logged.</td>
</tr>
</tbody>
</table>
User Events

The User tab displays user events with information for each event.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Details regarding the event.</td>
</tr>
<tr>
<td>Time</td>
<td>Time that the event was logged.</td>
</tr>
</tbody>
</table>

Reports Page

Use the Reports page to access various reports related to end users' desktop and application sessions.

**Important** The Desktop Health, Utilization, Session History, and Concurrency reports do not reflect user-related data until an hour has passed from the time you enabled monitoring user session information.

Select **Monitor > Reports** to open the Reports page, where you can view detailed information for the following categories. You can also manually refresh this page, filter your search, and export data to a Microsoft Excel worksheet.

**Note** If you have disabled monitoring user session information for utilization, trending, and historical analysis, the reports associated with that type of data are disabled and not visible on the Reports page. When that monitoring feature is disabled, the system collects such user session information for a limited period of time and hashes the username to enable real time administration while disabling historical and aggregated viewing of that user information. As a result, the reports that would display historical and aggregated viewing of that data, such as the Session History report, are not available.

The **Enable User Session Information** toggle for enabling or disabling monitoring user session information is located on the General Settings page (**Settings > General Settings**).

<table>
<thead>
<tr>
<th>Report Type</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Mapping</td>
<td>View details and sort by various categories, such as User name, Domain, Desktop Name, Desktop Model, Farm, and Mapping Type (User or Group).</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>This report is populated only for users that have at least one direct assignment to a desktop. In the Administration Console, you can choose individual users or user groups when making a desktop assignment. If a user has at least one assignment done as an individual user and zero or more assignments done as being part of the assigned group, this report reports all of that user's desktop assignments. However, if all of the user's desktop assignments are done using groups, that user's assignments are not reported in this report.</td>
</tr>
<tr>
<td>Desktop Mapping</td>
<td>View details and sort by various categories, such as Desktop Name, Model, Assignment Name, Type, Farm, Active User, Mapped Users, and Mapped User Groups.</td>
</tr>
<tr>
<td>Report Type</td>
<td>Details</td>
</tr>
<tr>
<td>-------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Desktop Health</td>
<td>View list of desktops, which can be filtered by assignment or error status. Click on a desktop to view report.</td>
</tr>
<tr>
<td></td>
<td>▪ For RDS desktops, the report includes CPU usage %, memory usage %, disk IOPS, and active/disconnected sessions.</td>
</tr>
<tr>
<td></td>
<td>▪ For VDI desktops, the report includes CPU usage %, memory usage %, disk IOPS, duration, bandwidth, and latency.</td>
</tr>
<tr>
<td>Utilization</td>
<td>View graphs for user and session trends, protocol and client usage, access type (internal or external), session duration, and service type. Can be filtered by assignment and time period.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> When <a href="#">Enable User Session Information</a> is turned off for your environment, the Unique User Summary feature of this report is not provided. The <a href="#">Enable User Session Information</a> is set in the General Settings page.</td>
</tr>
<tr>
<td>Session History</td>
<td>View session information by user, including last login time, session duration, weekly average use, and average session length. Can be filtered by time period.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> This report is not provided when <a href="#">Enable User Session Information</a> is turned off for your environment, as set in the General Settings page.</td>
</tr>
<tr>
<td>Concurrency</td>
<td>View per-assignment data for capacity, number of concurrent users, peak concurrency, and applications in use. Can be filtered by time period.</td>
</tr>
<tr>
<td>URL Configurations</td>
<td>View information for currently configured URL redirects. For more information, see <a href="#">Create a URL Redirection Configuration</a>.</td>
</tr>
</tbody>
</table>

**Notifications Page**

The Notifications page shows information regarding system notifications.

The Notifications page is available from the Monitor icon. You can perform these tasks.

- Use the Show filter to display notifications for only a certain period of time.
- View the total number of notifications.
- Use the Filter box to filter notifications.
- Refresh the list.
- Download information in the list in .xlsx format with the Export feature.

The Notifications page displays notifications with information for each one.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Icon indicates the type of notification.</td>
</tr>
<tr>
<td></td>
<td>▪ Blue &quot;i&quot; icon - information</td>
</tr>
<tr>
<td></td>
<td>▪ Yellow &quot;!&quot; icon - warning</td>
</tr>
<tr>
<td></td>
<td>▪ Red &quot;x&quot; icon - critical issue</td>
</tr>
<tr>
<td>Notification</td>
<td>Text of the notification.</td>
</tr>
<tr>
<td>Column</td>
<td>Description</td>
</tr>
<tr>
<td>--------</td>
<td>-------------</td>
</tr>
<tr>
<td>Status</td>
<td>Status of the notification. For example, Active or Dismissed.</td>
</tr>
<tr>
<td>Date</td>
<td>Date of notification.</td>
</tr>
</tbody>
</table>

**Note**  Notifications also appear in an abbreviated list format when you select the notifications icon ("bell" shape) at the top of the user interface page. You can double-click on a notification to view it on the Notifications page or select Show All to navigate to the Notifications page.
Assignments

On the Assignments page, you can create, edit, and delete assignments, and also update agent software for dedicated desktop assignments.

Click the Assign icon to access the Assignments page, where you can take these actions.

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>New</td>
<td>Create a new application or desktop assignment.</td>
</tr>
<tr>
<td>Edit</td>
<td>Select an assignment to make changes, or drill down to view summary and sessions information.</td>
</tr>
<tr>
<td>URL Redirection</td>
<td>Create a new assignment for a URL redirection configuration.</td>
</tr>
<tr>
<td>Update Agent</td>
<td>Update agents for dedicated desktop assignments.</td>
</tr>
<tr>
<td>Take Offline</td>
<td>For specific types of desktops assignments, allows you to take them off line for maintenance.</td>
</tr>
<tr>
<td>Delete</td>
<td>Delete an assignment.</td>
</tr>
<tr>
<td>Recover</td>
<td>Recover desktops that encountered an error during a previous image update.</td>
</tr>
<tr>
<td>Bring Online</td>
<td>Bring an offline desktop assignment online again.</td>
</tr>
</tbody>
</table>

Clicking on an assignment in the list opens a detail page showing summary information for the assignment. For some types of assignments, there are other tabs in addition to the Summary tab:

- Desktops - displays for dedicated and floating desktop assignments. See Manage Desktops in a Dedicated or Floating Desktop Assignment.
- System Activity and User Activity - display for dedicated and floating desktop assignments. See View System or User Activity for Assignments.
- Sessions - displays for native application assignments. See View System or User Activity for Assignments

The following topics provide additional information about data shown on the Assignments page:

- Types of Assignments - Describes values that display in the Type column.
- Capacity and Users Values for VDI Desktop Assignments - Describes values that display in the Capacity and Users columns.
This chapter includes the following topics:

- Types of Assignments
- Capacity and Users Values for VDI Desktop Assignments
- Create an Application Assignment
- Create a Dedicated or Floating VDI Desktop Assignment
- Create an RDSH Session Desktop Assignment
- Edit an Assignment
- Create a URL Redirection Configuration
- Edit Assignment Mode
- Update Agents for an Assignment
- Delete an Assignment
- Recover an Assignment
- Manage Desktops in a Dedicated or Floating Desktop Assignment
- View System or User Activity for Assignments
- Working with Nested Organizational Units

**Types of Assignments**

There are several types of assignments, as described in the table below. The type for each assignment appears in the Type column of the assignment list.
<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application</td>
<td>Use application assignments to assign Windows applications to groups. See Create an Application Assignment. Type displayed can be:</td>
</tr>
<tr>
<td></td>
<td>- Remote Applications - Assignment includes applications from servers in RDSH farms.</td>
</tr>
<tr>
<td></td>
<td>- Native Applications - Assignment includes AppStacks.</td>
</tr>
<tr>
<td>Desktops</td>
<td>Use desktop assignments to assign dedicated, floating, or RDSH-based virtual desktops to users and groups. See Create a Dedicated or Floating VDI Desktop Assignment and Create an RDSH Session Desktop Assignment. Type displayed can be:</td>
</tr>
<tr>
<td></td>
<td>- Dedicated Desktop - Traditional Clone</td>
</tr>
<tr>
<td></td>
<td>- Dedicated Desktop - Instant Clone</td>
</tr>
<tr>
<td></td>
<td>Note Dedicated Desktop - Instant Clone assignments can only be created in certain unusual configurations, and are not recommended. If you wish to create this type of assignment, consult your VMware representative first to confirm that you will be able to do so.</td>
</tr>
<tr>
<td></td>
<td>- Floating Desktop - Traditional Clone</td>
</tr>
<tr>
<td></td>
<td>- Floating Desktop - Instant Clone</td>
</tr>
<tr>
<td></td>
<td>- Session Desktop</td>
</tr>
<tr>
<td></td>
<td>Note Because a session desktop uses the traditional type of cloning by default, the Assignments page displays Session Desktop in the Type column for such assignments.</td>
</tr>
<tr>
<td></td>
<td>Definitions are as follows.</td>
</tr>
<tr>
<td></td>
<td>- Dedicated Desktop - In a dedicated desktop assignment, each user is assigned a specific remote desktop and returns to the same desktop at each login. Dedicated assignments require a one-to-one desktop-to-user relationship and should be sized based on the total user population. The primary use for dedicated desktop assignments is to ensure that the hostname of the desktop VM remains the same between sessions. Certain software packages might require this use for licensing.</td>
</tr>
<tr>
<td></td>
<td>- Floating Desktop - In a floating desktop assignment, a user might receive a different VM with a different machine name and/or hostname with each login. With floating desktop assignments, you can create desktops that shifts of users can use. Sizings should be based on the maximum number of concurrent users.</td>
</tr>
<tr>
<td></td>
<td>- Session Desktop - In a session desktop assignment, an RDSH-published desktop experience is shared across multiple users, that is, terminal services.</td>
</tr>
<tr>
<td></td>
<td>- Traditional Clone and Instant Clone - Type of cloning used for desktops. The option for selecting clone type is available while creating an image. The image selected for creating a desktop defines the desktop clone type. See Create an Image.</td>
</tr>
<tr>
<td></td>
<td>Note the following:</td>
</tr>
<tr>
<td></td>
<td>- A desktop can have multiple users assigned to it, but it can be used by only one user at a time.</td>
</tr>
<tr>
<td></td>
<td>- Desktops in floating desktop assignments do not provide persistence. You can configure persistence as part of an application assignment.</td>
</tr>
<tr>
<td></td>
<td>- Where possible, use floating desktop assignments because they cost less than dedicated desktop assignments and do not dedicate VM resources for each user.</td>
</tr>
<tr>
<td>URL Redirection Configuration</td>
<td>Use these assignments to assign URL handling rules to users. See Create a URL Redirection Configuration.</td>
</tr>
</tbody>
</table>
Capacity and Users Values for VDI Desktop Assignments

For dedicated and floating VDI desktop assignments, the capacity and user values shown in the respective columns on the Assignments page are calculated as described below.

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Capacity</td>
<td>Capacity represents the number of desktops involved in that dedicated or floating desktop assignment.</td>
</tr>
<tr>
<td>Users or user groups</td>
<td>Number of users or user groups currently mapped to the assignment. The actual number that is displayed depends on whether the assignment is mapped to a set of individual users, to a group or multiple groups, or to a combination of both.</td>
</tr>
</tbody>
</table>

**Note** For session desktop assignments and application assignments, the Assignment page’s Capacity column shows NA by default.

Create an Application Assignment

You can create an application assignment on the Assignments page.

**Procedure**

1. Click the **Assign** icon.
   The Assignments page displays.

2. Click **New**.

3. Click the **Get Started** button under Applications.

4. On the Definition tab, select a type for the assignment.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remote</td>
<td>Assignment includes applications from your RDSH farms.</td>
</tr>
<tr>
<td>Native</td>
<td>Assignment includes AppStacks.</td>
</tr>
</tbody>
</table>

**Note** The fields displayed on this tab will differ depending on the type you select.
If you selected Native, enter information in the fields as described below, click Next, and then proceed to Step 9 below.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assignment Name</td>
<td>Unique name for the assignment.</td>
</tr>
<tr>
<td>OS</td>
<td>Select the correct OS from the drop-down menu. This OS must be the same OS as the OS used to capture the applications.</td>
</tr>
<tr>
<td>Computer Name Prefix</td>
<td>(Optional) Enter a prefix. Entering a prefix limits access to the application assignment to authorized users who log in to a desktop assignment that has the same prefix at the beginning of its name. If you leave this option blank, all authorized users can access the new application assignment regardless of the desktop assignments they are logged in to.</td>
</tr>
</tbody>
</table>

If you selected Remote, enter a unique name for the assignment and the proceed to the next step.

7 On the Applications tab, select the remote applications or AppStacks to include in the assignment, and click Next.

The displayed list reflects whether you selected Remote or Native for the application type in the previous steps. If you had selected Remote for the application type, the applications you select here can be from different farms.

8 On the Users tab, start typing the name of a user or group in the text box, and then click the name in the list to select it.

9 (Optional) Repeat the previous step to select additional users or groups.

10 Click Next.

11 On the Summary tab, review the information on and if it is correct, click Submit. If not, click Back to return to previous tabs and edit your information.

**Create a Dedicated or Floating VDI Desktop Assignment**

You create VDI desktop assignments from the Assignments page.

Use these steps to assign a dedicated or floating VDI desktop to your end users. To assign a session-based (RDSH) desktop, see the steps in Create an RDSH Session Desktop Assignment.

**Procedure**

1 Click the Assign icon.

The Assignments page displays.

2 Click New.

3 Click the Get Started button under Desktops.

The Assign Desktops dialog displays.
4 Select either Dedicated or Floating to create an assignment for a VDI desktop. For information on types of desktop assignments see Types of Assignments. For the steps on creating a session-based desktop, see Create an RDSH Session Desktop Assignment.

**Note** There will be some variation in the fields displayed on the screen, depending on the type of desktop assignment you are creating. These variations are noted in the following steps.

5 Enter information for Fixed Attributes.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pod</td>
<td>This option only displays if the data center is configured with multiple pods. You can only create assignments from images in the same pod.</td>
</tr>
<tr>
<td>Desktop Model</td>
<td>Select model from the drop-down list.</td>
</tr>
<tr>
<td>Domain</td>
<td>[Traditional Clone images only] Select domain from the drop-down list.</td>
</tr>
<tr>
<td>Join Domain</td>
<td>[Traditional Clone images only] Leave default setting (Yes).</td>
</tr>
</tbody>
</table>

6 Enter information for the Flexible Attributes displayed.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Image</td>
<td>Select an image from the list. In the list, the acronym for the image type appears at the beginning of the image name. For example, [IC] image1 is an Instant clone image and [TC] image 2 is a Traditional Clone image. For dedicated desktop assignments, Instant Clone images will not display for most users. It is not recommended to create this type of assignment, but if you wish to do so, consult your VMware representative first to confirm that your system is configured to allow this. For dedicated and floating desktop assignments, RDSH role-enabled images will not be listed, since there is no reason that users would want to create dedicated or floating desktop assignments from those images. RDSH role-enabled images are used for session desktop assignments.</td>
</tr>
<tr>
<td>Assignment Name</td>
<td>A unique name for the new assignment.</td>
</tr>
<tr>
<td>Default Protocol</td>
<td>Select Blast (HTML Access) or PCoIP.</td>
</tr>
<tr>
<td>Preferred Client Type</td>
<td>Select Browser or Horizon Client.</td>
</tr>
<tr>
<td>Capacity</td>
<td>Number of desktops required in the assignment.</td>
</tr>
</tbody>
</table>

7 Under Flexible Attributes, expand Advanced Properties and enter required information.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VM Names</td>
<td>Name for all virtual machines or guest desktops in this assignment, which will have a number appended to it, for example, win7-1, win7-2, win7-Floating. The name must start with a letter and can contain only letters, dashes, and numbers. This value is prefilled based on the assignment name.</td>
</tr>
<tr>
<td>Computer OU</td>
<td>Active Directory (AD) Organizational Unit where VMs are located. For example, OU=NestedOrgName,OU=RootOrgName,DC=DomainComponent,DC=eng, and so on. The entries must be comma-separated with no spaces in between. For more information about Active Directory, see Working with Nested Organizational Units.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Run Once Script</td>
<td><em>(Optional)</em> Location of scripts that should run after system preparation completes.</td>
</tr>
<tr>
<td>Session Timeout Interval</td>
<td>The timeout value for end user sessions to the desktops. The default is seven days (10,080 minutes). The maximum value is 99,999 minutes, approximately 69 days. <strong>Note</strong> If no user activity occurs before the timeout interval is reached, a message indicates that the user will be logged off if they do not click <strong>OK</strong> in the next 30 seconds. If the logoff occurs, any unsaved documents are lost. If you are assigning a timeout value for dedicated desktops, you can specify the maximum value. If you have a large timeout interval set for floating desktops, the desktops do not reset as quickly if they are not in use. This configuration might result in the pool of available desktops running out, and users seeing failure messages.</td>
</tr>
<tr>
<td>Hotplug Enabled</td>
<td>This setting enables/disables the HotPlug functionality for desktops in an assignment. When this is set to No (default setting), network adapters do not appear in the Quick Add/Remove area. This makes it more difficult for users to put their VMs into an unusable state.</td>
</tr>
</tbody>
</table>

8. Click **Next**.

9. Select an image from the list.

   In the list, the acronym for the cloning type used on the image appears at the beginning of the image name. For example, 'IC\ image1' is an Instant clone image and 'TC\ image 2' is a Traditional Clone image.

10. Click **Next**.

11. On the Active Directory Search page, start typing the name of a user or group from your Active Directory.

12. Select a user or group from the list.

13. *(Optional)* Search for and select additional users or groups, and click **Next**.

   If you assign a dedicated desktop to more than one user, a warning message appears to verify if this is the intended configuration. The configuration is supported, but the users would share the desktop and only one can use it at any one time.

14. On the Summary page, confirm that the displayed information is correct and click **Submit**.

15. Click the **Assign** icon to see your new assignment.

**Create an RDSH Session Desktop Assignment**

You create session desktop assignments using the Assignments page.

For general information about desktop assignments, see **Types of Assignments**.
Prerequisites

Verify you have the following items:

- The Farms page lists at least one farm of remote desktops type. Only farms configured to deliver remote desktops can be used for a session desktop assignment.
- The farm you want to use is in the node from which you want to deliver the session desktops.
- The farm is not already used in an assignment. A farm configured to deliver remote desktops cannot be used in more than one session desktop assignment. To verify whether the farm you want to use is already used in a session desktop assignment, look in the Assignment page’s Farms column and see if the farm is listed. If it is listed, then it is already being used in a session desktop assignment and you will have to create a new farm.

Procedure

1. Start the New Assignment workflow by clicking **Assign** and clicking **New**.
2. In the New Assignment start screen, click the Desktops icon.

   The New Desktop Assignment window opens to the first wizard step.

3. On the wizard's Definition step, click **Session**.
4 Complete the selections on the Definition step and then click Next.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pod</td>
<td>This option only displays if your data center is configured with multiple pods. Pods contain specific assignable images and server model capacities for assignments. You can only create assignments from images in the same pod.</td>
</tr>
<tr>
<td>Farm</td>
<td>Select the farm that has the configured RDS-enabled image that you want to assign to the end users. Only farms that are in the selected node and which not already involved in existing session desktop assignments are available for selection.</td>
</tr>
<tr>
<td>Assignment Name</td>
<td>Type a friendly name for this assignment. The end users see this name when they go to access their assigned desktop. For example, when an end user launches Horizon Client to go to an assigned desktop, this name is the one displayed in Horizon Client. The name must contain only letters, hyphens, and numbers. Spaces are not allowed. The name cannot start with a non-alphabetic character.</td>
</tr>
</tbody>
</table>

5 On the Users step, search for users and groups in your registered Active Directory domains, select the ones you want to give this session desktop assignment, and then click Next.

6 On the Summary step, review the configuration and then click Submit.

The system begins the process of configuring the farm's server instances to provide session desktops to the selected users. On the Assignments page, the Status column reflects the current progress.

**Edit an Assignment**

You can change assignment settings such as capacity and assigned users.

**Procedure**

1 On the Assignments page, select the assignment to edit and click Edit.

2 Make your changes and click Submit.

   **Note** If you edit the capacity of a desktop assignment, it takes a few minutes for the system to reflect the change.

For instructions on filling in the fields in the wizard, see the topic for creating the type of assignment you are editing (Create an Application Assignment or Create a Dedicated or Floating VDI Desktop Assignment).
Create a URL Redirection Configuration

Use these configurations in Horizon Cloud to define URL handling rules where the Horizon Client redirects URLs from the end user's client machine to a desktop or application provided by your Horizon Cloud environment. A URL redirection configuration gives the Horizon Client information about which URLs should be handled by one of the end user's assigned Horizon Cloud desktops or applications instead of being opened by the user's local system.

**Note** The Horizon Cloud Administration Console provides a user interface for you to configure client-to-agent URL redirection. To configure agent-to-client URL redirection, you must use group policy settings as described in Configuring Agent-to-Client Redirection. The steps below are for configuring client-to-agent URL redirection.

The Horizon Client fetches an end user's assigned URL redirection configurations when the user logs in to the Horizon Client on their local device. Then when that user attempts to open a link in a local document or file and the link matches a URL pattern rule in the configuration, Horizon Client determines the appropriate handler to use. The handlers are specified opens the user's assigned desktop or application to handle the URL link, as determined by the appropriate handler you specified in the URL redirection configuration. If the URL redirection handler specifies to use a desktop, the desktop's default application for the link's specified protocol processes the URL. If the handler specifies to use an application, the user's assigned application processes the URL. If the user is not entitled to the desktop or application specified in the handler, Horizon Client displays a message to the user, unless you have specified **Strict Match** as **No** for the handler.

In the scenario where **Strict Match** is set to **No**, the system locates a resource to use based on this fall-back behavior:

1. The system searches the user's assignments using a substring match of the target resource specified for the handler. If the system finds an assignment that matches the substring, that assigned desktop or application is used to open the link.

2. When the handler's **Resource Type** is set to **Application**, if the search for a substring match fails, the system searches the user's application assignments for an assigned application that can handle the protocol specified in the handler's **Scheme** field.

**Note** This step in the fall-back behavior only applies for applications. If the **Resource Type** is set to **Desktops**, this step is skipped.
3. If the system cannot locate a resource in the user's assignments that can handle the protocol, Horizon Client displays a message to the user.

**Important** The user's Horizon Client must be installed with the URL_FILTERING_ENABLED=1 option to give the client the capability to handle the URL redirection feature. For details, see the Installing Horizon Client for Windows with the URL Content Redirection Feature topic in the VMware Horizon 7 documentation.

When your environment is integrated with VMware Identity Manager™, the user must have opened at least one application using Horizon Client before the URL redirection feature can work for that user. By opening at least one application using the **Open in Client** option, the user's assigned URL redirection configuration is loaded into the client device's registry where Horizon Client can get the configuration values.

A user can be assigned more than one URL redirection configuration, where those configurations have the **Active** toggle set to Yes. To avoid potential conflicts between rules from different configurations, when the user logs in to Horizon Client, the system:

- Sets only one configuration in effect, even when that user has more than one active assigned configuration.
- Uses the URL redirection configuration that is alphabetically first as the configuration in effect for the user.

**Prerequisites**

Verify that you have met the following prerequisites before using the Administration Console to create a URL redirection configurations:

- The Horizon agent in the base image used by the farm was installed using the URL_FILTERING_ENABLED=1 parameter on the command line.
- Your Horizon Cloud inventory has the session desktops and remote applications that you intend to use in the configuration.

**Procedure**

1. On the Assignments page, click **URL Redirection**.

   The New URL Redirection Configuration wizard opens to its first step.

2. In the Definition step's General Settings section, configure the general settings and then scroll to the Rules section.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a friendly name for this configuration.</td>
</tr>
<tr>
<td>Active</td>
<td>Select <strong>Yes</strong> to make this configuration active.</td>
</tr>
<tr>
<td>Description</td>
<td>Optionally enter a description for the configuration.</td>
</tr>
</tbody>
</table>
3 In the Rules section, create a list of URL patterns that this configuration will tell Horizon Client to intercept on the client system.

   a In the **URL Pattern** field, type a quoted string that specifies the URL matching pattern to be intercepted.
      
      You must include the protocol prefix, like `https://`. You can use wildcards to specify a URL pattern that matches multiple URLs.
      
      For example:
      
      - If you type "http://google.*", all URLs that include the text `google` are intercepted.
      - If you type `.*/` (period asterisk), all URLs are intercepted (matches all).
      - If you type "mailto://.*.example.com" all URLs that contain the text `mailto://.*.example.com` are intercepted.
      
   b Click **Add** to add the URL pattern to the list of rules.
   
   a Repeat the steps to add more URL matching patterns.

4 Click **Next** to proceed to the next wizard step.
On the Configuration step, define the set of handlers that determine which target inventory resource should handle various protocols.

A handler defines which of the user's entitled desktops or applications should handle that specific protocol. For example, if the user opens a Microsoft Word document that has a `mailto` hypertext link and the user clicks on that link in the document, the handler defines what entitled application should handle the request, such as Microsoft Outlook or Mozilla Thunderbird.

a Click **New**.

b In the handler window, configure the settings and click **Save**.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name</strong></td>
<td>Enter a name for the handler.</td>
</tr>
<tr>
<td><strong>Scheme</strong></td>
<td>Enter the protocol to which this handler applies, such as <code>http</code>, <code>https</code>, <code>mailto</code>, <code>callto</code>, and so on.</td>
</tr>
<tr>
<td><strong>Resource Type</strong></td>
<td>Select whether a desktop or application is to handle the specified protocol.</td>
</tr>
<tr>
<td><strong>Target Resource</strong></td>
<td>Enter the name of the target resource in your Horizon Cloud inventory that you want handling the protocol specified in the <strong>Scheme</strong> field.</td>
</tr>
<tr>
<td><strong>Strict Match</strong></td>
<td>Select <strong>Yes</strong> to force an exact match between the name specified in the <strong>Target Resource</strong> field and the names of the user's available entitled session desktops or remote applications. Select <strong>No</strong> if you want the system to use its fall-back behavior to support the situation where an end user does not have an assignment for a resource with the exact name specified in the <strong>Target Resource</strong> field. For example, when the <strong>Resource Type</strong> is set to Applications and you specify Microsoft Outlook as the target resource to handle the <code>mailto</code> protocol, but the user does not have an assignment for any Microsoft Outlook applications, when <strong>Strict Match</strong> is set to No, the system will search for a compatible application assigned to that user to handle the <code>mailto</code> protocol, such as Mozilla Thunderbird.</td>
</tr>
</tbody>
</table>

c Repeat the steps to add more handlers.

6 Click **Next** to proceed to the next wizard step.

7 Search for and select the users and groups for this URL redirection assignment and click **Next**.

8 Review the summarized information and click **Submit**.

**Understanding What URL Content Redirection Is**

Generally speaking, the URL content redirection feature supports redirection from a remote desktop or application to a client, and from a client to a remote desktop or application.
Redirection from a remote desktop or application to a client is called agent-to-client redirection. Redirection from a client to a remote desktop or application is called client-to-agent redirection.

**Agent-to-client redirection**

With agent-to-client redirection, Horizon Agent sends the URL to Horizon Client, which opens the default application for the protocol in the URL on the client machine. For details about configuring agent-to-client redirection in Horizon Cloud, see Configuring Agent-to-Client Redirection.

**Client-to-agent redirection**

With client-to-agent redirection, Horizon Client opens a remote desktop or remote application that you specified to handle the URL. For details about configuring client-to-agent redirection in Horizon Cloud, see Create a URL Redirection Configuration.

You can redirect some URLs from a remote desktop or application to a client, and redirect other URLs from a client to a remote desktop or application. You can redirect any number of protocols, including HTTP, HTTPS, mailto, and callto.

### Configuring Agent-to-Client Redirection

With agent-to-client redirection, Horizon Agent sends the URL to Horizon Client, which opens the default application for the protocol in the URL.

To enable agent-to-client redirection, perform the following configuration tasks.

- Ensure the URL content redirection feature is enabled in Horizon Agent in the master image VM, as described in the prerequisites section in Create a URL Redirection Configuration.
- Apply the URL Content Redirection group policy settings to your remote desktops and applications. See Add the URL Content Redirection ADMX Template to a GPO.
- Configure group policy settings to indicate, for each protocol, how the Horizon Agent should redirect the URL. See URL Content Redirection Group Policy Settings.

### Add the URL Content Redirection ADMX Template to a GPO

The URL Content Redirection ADMX template file, called urlRedirection.admx, contains settings that enable you to control whether a URL link is opened on the client (agent-to-client redirection) or in a remote desktop or application (client-to-agent redirection).

To apply the URL Content Redirection group policy settings to your remote desktops and applications, add the ADMX template file to GPOs on your Active Directory server. For rules regarding URL links clicked in a remote desktop or application, the GPOs must be linked to the OU that contains your virtual desktops and RDS hosts.

You can also apply the group policy settings to a GPO that is linked to the OU that contains your Windows client computers, but the preferred method for configuring client-to-agent redirection is to use the vdmutil command-line utility. Because macOS does not support GPOs, you must use vmdutil if you have Mac clients.
Prerequisites

- Verify that the URL content redirection feature is included when Horizon Agent is installed in the master image VM, as described in Create a URL Redirection Configuration.
- Verify that Active Directory GPOs are created for the URL Content Redirection group policy settings.
- Verify that the MMC and the Group Policy Management Editor snap-in are available on your Active Directory server.

Procedure

1. Download the Horizon 7 GPO Bundle ZIP file from the VMware download site at my.vmware.com/web/vmware/downloads. The file has a name in the form VMware-Horizon-Extras-Bundle-x.x.x-yyyyyyy.zip where x.x.x is the version and yyyyyyy is the build number. All ADMX files that provide group policy settings for the product are available in this file.

2. Unzip that ZIP file and copy the URL Content Redirection ADMX file to your Active Directory server.
   a. Copy the urlRedirection.admx file to the C:\Windows\PolicyDefinitions folder.
   b. Copy the urlRedirection.adml language resource file to the appropriate subfolder in C:\Windows\PolicyDefinitions. For example, for the EN locale, copy the urlRedirection.adml file to the C:\Windows\PolicyDefinitions\en-US folder.

3. On your Active Directory server, open the Group Policy Management Editor. The URL Content Redirection group policy settings are installed in Computer Configuration > Policies > Administrative Templates > VMware Horizon URL Redirection.

What to do next

Configure the group policy settings in your Active Directory server. For descriptions of the settings, see URL Content Redirection Group Policy Settings.

URL Content Redirection Group Policy Settings

The URL Content Redirection template file contains group policy settings that enable you to create rules for configuring the agent-to-client redirection capability for your Horizon Cloud environment. The template file contains only Computer Configuration settings. All of the settings are in the VMware Horizon URL Redirection folder in the Group Policy Management Editor.

**Important** Even though the URL Content Redirection template file contains group policy settings related to client-to-agent redirection, you do not use group policy settings to configure client-to-agent redirection in Horizon Cloud. In Horizon Cloud, you use the Administration Console to create the rules for client-to-agent redirection. You create rules for client-to-agent redirection when you create a URL redirection assignment in the Administration Console. For detailed steps, see Create a URL Redirection Configuration.
The following table describes the group policy settings available in the URL Content Redirection template file.

### Table 6-1. URL Content Redirection Group Policy Settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Properties</th>
</tr>
</thead>
<tbody>
<tr>
<td>IE Policy: Prevent users from changing URL Redirection plugin loading behavior</td>
<td>Determines whether users can disable the URL Content Redirection feature. This setting is not configured by default.</td>
</tr>
<tr>
<td>IE Policy: Automatically enable URL Redirection plugin</td>
<td>Determines whether newly installed Internet Explorer plug-ins are automatically activated. This setting is not configured by default.</td>
</tr>
<tr>
<td>Url Redirection Enabled</td>
<td>Determines whether the URL Content Redirection feature is enabled. You can use this setting to disable the URL Content Redirection feature even if the feature has been installed in the client or agent. This setting is not configured by default.</td>
</tr>
</tbody>
</table>
### Table 6-1. URL Content Redirection Group Policy Settings (Continued)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Properties</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Url Redirection Protocol 'http'</strong></td>
<td>For all URLs that use the HTTP protocol, specifies the URLs that should be redirected. This setting has the following options:</td>
</tr>
<tr>
<td></td>
<td>- <strong>brokerHostname</strong> - IP address or fully qualified name of the Connection Server host to use when redirecting URLs to a remote desktop or application.</td>
</tr>
<tr>
<td></td>
<td>- <strong>remoteItem</strong> - display name of the remote desktop or application pool that can handle the URLs specified in <strong>agentRules</strong>.</td>
</tr>
<tr>
<td></td>
<td>- <strong>clientRules</strong> - the URLs that should be redirected to the client. For example, if you set <strong>clientRules</strong> to <code>*.mycompany.com</code>, all URLs that include the text <code>mycompany.com</code> are redirected to the Windows-based client and are opened in the default browser on the client.</td>
</tr>
<tr>
<td></td>
<td>- <strong>agentRules</strong> - the URLs that should be redirected to the remote desktop or application specified in <strong>remoteItem</strong>. For example, if you set <strong>agentRules</strong> to <code>*.mycompany.com</code>, all URLs that include <code>mycompany.com</code> are redirected to the remote desktop or application.</td>
</tr>
<tr>
<td></td>
<td>When you create agent rules, you must also use the <strong>brokerHostname</strong> option to specify the IP address or fully qualified domain name of the Connection Server host, and the <strong>remoteItem</strong> option to specify the display name of the desktop or application pool.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> The preferred method for configuring client rules is to use the vdmutil command-line utility.</td>
</tr>
</tbody>
</table>

This setting is enabled by default.

<table>
<thead>
<tr>
<th><strong>Url Redirection Protocol '...]'</strong></th>
<th>Use this setting for any protocol other than HTTP, such as HTTPS, email, or callto.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>The options are the same as for <strong>Url Redirection Protocol 'http'</strong>.</td>
</tr>
<tr>
<td></td>
<td>If you do not need to configure other protocols, you can delete or comment out this entry before adding the URL Content Redirection template file to Active Directory.</td>
</tr>
<tr>
<td></td>
<td>As a best practice, configure the same redirection settings for the HTTP and HTTPS protocols. That way, if a user types a partial URL into Internet Explorer, such as <code>mycompany.com</code>, and that site automatically redirects from HTTP to HTTPS, the URL Content Redirection feature will work as expected. In this example, if you set a rule for HTTPS but do not set the same redirection setting for HTTP, the partial URL that the user types is not redirected.</td>
</tr>
<tr>
<td></td>
<td>This setting is not configured by default.</td>
</tr>
</tbody>
</table>

### Edit Assignment Mode

You can take assignments offline for maintenance and bring them back online using the Edit Assignment Mode setting. Setting an Assignment to offline mode will prevent users from logging into the assignment desktops/applications. The setting also allows you to configure a custom maintenance notice for the assignment.
You can perform the following tasks using the Edit Assignment Mode setting.

- Take an assignment offline:
  a. On the Assignments page, select the assignment and click the **Edit Assignment Mode** button at the top of the page.
     The Edit Assignment Mode dialog appears.
  b. Change the Assignment Mode setting to Offline.
  c. Click **Save**.

- Bring an assignment online:
  a. On the Assignments page, select the assignment and click the **Edit Assignment Mode** button at the top of the page.
     The Edit Assignment Mode dialog appears.
  b. Change the Assignment Mode setting to Online.
  c. Click **Save**.

### Update Agents for an Assignment

Use the Update Agent Software feature to update agents for Dedicated Desktop - Traditional Clone assignments.

**Note** You can also update agent software for a Dedicated Desktop - Instant Clone assignment by updating the image and pushing changes to the assignment. This process is described in Update Agent Software for an Image.

The agent update feature allows automated update of all the agents in an assignment in a single operation.

- The system makes regular contact with the VMware CDS software distribution network and downloads agent updates automatically to a file share that you have set up on a local machine. The update files are then automatically imported into the system and made available to assignments.

- The availability of updates is indicated on the Assignments page, where you can apply them to assignments. When you initiate the upgrade task on an assignment, all VMs in the assignment are be updated as part of that task.

- Your VMware representative can adjust the interval between scans for new agents and the wait time for scans after tenant startup if you request it.

**Prerequisites**

- You must have created an Agents file share and added it to Horizon Cloud. This means that you select Agents for the file share type when you create the file share. Agents file shares are used only for importing agent update files. See Managing File Shares.

- The assignment must already have DaaS Agent 16.6.0.4408091 or higher in order to perform a DaaS Agent update.
The assignment must already have Horizon Agent 7.0.3.4612900 or higher in order to perform a Horizon Agent update.

Procedure

1. Click Assign.

The Assignments page displays, with a blue dot appearing next to the name of any assignment that has agent updates available.

- If you hover over a blue dot, a popup displays indicating the agent updates available for that assignment.
- The system selects the latest versions of each agent by default, but you can open each drop-down to view all available versions.

2. Select the check boxes for one or more assignments. By selecting multiple assignments, you can update all of them to a common set of agent versions.

3. Click Update Agent Software.

The Agent Update dialog displays.

4. On the Software tab, select the agent(s) to update and click Next.

5. On the Agreements tab, select the Agree radio button for each agreement you wish to accept and click Next. The system skips the update for any item for which you do not accept the agreement.

6. (Optional) On the Command Line tab, add any command line options. For details regarding command line options, see the documentation for the relevant agent.

   Note: There are currently no command line options available for the DaaS Agent.

7. Click Finish.

A message displays at the top of the page indicating that the update has started.

Note the following:

- Desktops are updated in batches, which cannot be larger than 30. If the assignment has 30 or fewer desktops, all desktops in the assignment will be updated together. Your VMware representative can adjust the batch size if you request it.
- If a desktop has an active session, the user will be warned five minutes before the update occurs.
- If a user attempts to login into a desktop that is being updated, the login will be unsuccessful and the user will receive a message that the desktop is not available.

You can view the progress of the update task by selecting Monitor > Activity. The task description indicate the agent being updated and the assignment on which the update is being performed. If the task is not successful within 24 hours, it fails.

Delete an Assignment

You can delete assignments if they are no longer needed.
**Prerequisites**

An assignment can be deleted only if it contains no virtual machines.

- To delete a dedicated desktop assignment, first delete the virtual machines from the Assignment page.
- To delete a floating desktop assignment, first set the assignment size to zero.

**Procedure**

1. Select the assignment to delete and click **Delete**.
2. Click **Delete** in the confirmation dialog box to permanently delete the assignment.

**Recover an Assignment**

You can recover desktops that encountered an error during a previous image update.

**Procedure**

1. Select the assignment to recover.
2. Click **Recover**.

**Manage Desktops in a Dedicated or Floating Desktop Assignment**

You can manage desktops in dedicated and floating desktop assignments.

**Note**  For session desktop assignments, the assignments are only used for entitling access to the RDS-based desktop, and not for management of the desktops. To manage session desktops, you manage the servers and sessions in the underlying farm. See **Managing Farms in Horizon Cloud**.

**Procedure**

1. Click the **Assign** icon.
   
   The Assignments page displays.

2. Click the name of an assignment on the list.
   
   The assignments details page displays.

3. Click **Desktops** at the top of the page.
   
   The Desktops tab displays, showing a list of desktops for the assignment. You can filter, refresh, and export the list using the controls to the top right of the page.

   You can perform the following actions by clicking one of the buttons at the top of the page.

   **Note**  Desktop status must be green to perform these actions.
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Shutdown</td>
<td>Shuts down the desktop(s).</td>
</tr>
<tr>
<td></td>
<td>- You can select more than one desktop at a time.</td>
</tr>
<tr>
<td></td>
<td>- You can only shut down VMs that do not have active user sessions.</td>
</tr>
<tr>
<td>Restart</td>
<td>Performs a ‘graceful’ restart of the VM(s). You can select more than one desktop at a time. If this does not work, it may be necessary to use the Reset option (see below).</td>
</tr>
<tr>
<td>Assign</td>
<td>[Dedicated desktop assignments only] Assigns dedicated desktop to a particular user. Click the button and then search for the user in the Active Directory.</td>
</tr>
</tbody>
</table>

You can perform the following actions by clicking the "..." button and making a selection from the drop-down menu.

| Rename      | [Dedicated desktop assignments only] Renames the selected desktop.                                                                |
| Unassign    | [Dedicated desktop assignments only] Unassigns the selected desktop from user.                                                |
| Delete      | [Dedicated desktop assignments only] Deletes the selected desktop.                                                             |
| Suspend     |Suspends the selected desktop(s). You can select more than one desktop at a time.                                             |
| Resume      |Resumes operation of the selected desktop(s). You can select more than one desktop at a time.                                   |
| Power On    | [Traditional clone assignments only] Powers on the selected desktop(s). You can select more than one desktop at a time.       |
| Power Off   | [Traditional clone assignments only] Powers off the selected desktop(s). You can select more than one desktop at a time.      |
| Reset       | Performs a hard reset of the VM(s). You can select more than one server at a time. In the case of a hung VM, it is recommended that you first try using the Restart option (see above). |
| Log Off     | Logs the currently connected user off the selected desktop.                                                                   |
| Disconnect  | Disconnects the currently connected user from the selected desktop.                                                             |
| Launch Console | Launches a console for the selected desktop. This option is disabled if the VM is powered off or if more than one VM is selected. |
| Rebuild     | [Floating desktop assignments only] Deletes and recreates the selected desktop. Use this option for desktop VMs that have become corrupted or otherwise non-operational. |
| Convert to Image | Converts the selected desktop to an image.                                                                                       |

**Note** You cannot convert a VM to an image if it is currently being used as an appliance.

### View System or User Activity for Assignments

You can use an assignment's details page to view system or user activity for dedicated and floating desktop assignments. You can also view session activity for a native application assignment.
Use these steps to view system or user activity for dedicated desktop and floating desktop assignments, and session activity for native application assignments. For session desktop assignments, you view the system and user activity using the details page for the underlying farm. See Managing Farms in Horizon Cloud for details.

**Procedure**

1. Click the **Assign** icon. The Assignments page displays.
2. Click the name of an assignment on the list. The assignments details page displays.
3. Click one of the options, depending on whether the assignment is a dedicated desktop, floating desktop, or a native application assignment.
   - For a dedicated desktop or floating desktop assignment, click **System Activity** or **User Activity**. The activity tab displays, showing a list of recent activity for the assignment. You can select from the Shown drop-down menu to adjust the time frame for the list, or filter, refresh, and export the list using the controls on the top right of the page.
   - For a native application assignment, click **Sessions**.

**Working with Nested Organizational Units**

Add desktops to a nested Organization Unit (OU).

When you create a desktop assignment, you can specify a domain OU in the Computer OU field. You cannot specify a nested OU. You must locate the nested OU information, then manually enter it in the Computer OU field.

**Procedure**

1. Open **Active Directory Users and Computers**.
2. Select **View > Advanced features (Enabled Advanced features)**.
3. Navigate to the Organizational Unit where the desktops will be placed.
4. Right-click and select **Properties**.
5. Click the **Attribute editor** and select distinguishedName.
6. Click **View**.
7. Enter the distinguished name information in the Computer OU field on the Desktop Assignment page. Only the **OU=** part of the string is required. The **DC=** part is optional.
The Applications page shows all of the applications available for assignments.

Click the **Inventory** icon and select **Applications** to access the Applications page.

There are three types of applications:

- Native applications are imported in AppStacks. This import function is not on the Applications page. See *Import Applications Using App Volumes*.

  When multiple applications are imported together as an AppStack, the AppStack displays as a single item in the Applications list, with a number attached to its icon indicating the number of applications in it. You can hover over the name in the Application column to see a list of applications in the AppStack (up to 10 items).

- Remote applications are those imported from an RDS farm. You add third-party user applications to the RDS image before publishing that image to Horizon Cloud. You can either automatically scan your farms to add their applications to your applications inventory or manually add applications from the farm.

- Custom applications are applications in the RDS farms' servers that you manually add into the inventory by using the **New** button on the Applications page and the **Manually from Farm** choice. Even though the best practice is to use the automated way, the manual method can be useful for some unique situations, such as for adding applications that are invoked from the command prompt or which cannot be auto-detected in a Windows operating system.

You can take the following actions on the Applications page:

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>New</td>
<td>Add a Remote or Custom Application.</td>
</tr>
<tr>
<td>Edit</td>
<td>Select an application to make changes.</td>
</tr>
<tr>
<td>Delete</td>
<td>Delete an application.</td>
</tr>
<tr>
<td>Rename</td>
<td>Rename an application.</td>
</tr>
</tbody>
</table>

This chapter includes the following topics:

- Importing New Applications from an RDSH Farm Using Auto-Scan from Farm
- Manually Adding Custom Applications from an RDSH Farm
- Edit an Application
Deleting an Application

Rename an Application

Hide an Application

Unhide an Application

Import Applications Using App Volumes

Importing New Applications from an RDSH Farm Using Auto-Scan from Farm

You make remote applications available for user assignments by importing them from an RDSH applications farm.

If you have more than one applications farm in your environment, repeat these steps to import the applications you want from each of those farms.

Prerequisites

Verify that you have at least one applications farm in your inventory by navigating to Inventory > Farms.

Procedure

1. On the Applications page, click New.

2. In the start screen, click Auto-Scan from Farm.
   The wizard opens to its first step.

3. Select the applications farm and click Next to proceed to the next step.
   When you click Next, the system scans the selected farm for applications and then displays them for you to select.

4. Select the applications that you want to add to your application catalog.
   This wizard step displays the applications that the system's auto-scan process found in the RDS-enabled Windows server operating system used for the farm's RDS servers.
5 Click **Next** to proceed to the next wizard step.

6 (Optional) Customize some of the configurable options for the applications you selected, and then click **Next** to proceed to the next wizard step.

7 Review the summary and click **Submit**.

The system adds the selected applications to the application catalog in your Horizon Cloud inventory.

**What to do next**

Repeat the steps to import the applications you want from your other farms.

### Manually Adding Custom Applications from an RDSH Farm

Some applications cannot be automatically detected by scanning the farm. You can manually add those applications to your Horizon Cloud applications catalog.

If you have more than one such application, repeat these steps to add the applications you want.

**Prerequisites**

Verify that you have at least one applications farm in your inventory by navigating to **Inventory > Farms**.

**Procedure**

1 On the Applications page, click **New**.

2 In the start screen, click **Manually from Farm**.

3 In the Properties section, specify the following values.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Unique name for the application.</td>
</tr>
<tr>
<td>Display Name</td>
<td>Name for the application that you want displayed to end users when they see the application in their clients, such as in Horizon Client or Workspace ONE.</td>
</tr>
</tbody>
</table>
**Pod**
This option only displays if your data center is configured with multiple pods. Select a pod to filter the set of farms displayed in the Farm list.

**Farm**
Select the farm that has the RDSH server VM from which you want to add the application.

**Application Path**
Specify the path to the application in the RDSH server VM's operating system.

**Icon File**
Optional: Upload a PNG file (32 x 32 pixels) to use as the application's icon.

4 In the Advanced Properties section, specify these optional settings.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application available on Farm</td>
<td>Select <strong>Yes</strong> to have the system validate the application path. If the application is not located on the farm at that path, select <strong>No</strong> so that the system does not attempt to look for the application. For example, if an application is stored in the local directory in the server VM, you would select <strong>No</strong> so that the system does not try to find the application there.</td>
</tr>
<tr>
<td>Version</td>
<td>Optional: Version number of the application</td>
</tr>
<tr>
<td>Publisher</td>
<td>Optional: Publisher of the application</td>
</tr>
<tr>
<td>Start Folder</td>
<td>Specify the location in the RDS server VM's Windows operating system that you want the remote application to use as its start folder.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> If you specify a LNK file in the Application Path that specifies its own start directory, the system does not use the location specified here.</td>
</tr>
<tr>
<td>Parameters</td>
<td>Specify any command line parameters you want used when the remote application is launched.</td>
</tr>
</tbody>
</table>

5 Click **Submit**.

The system adds an entry for the application to the Applications page.

**What to do next**
Repeat the steps for any applications you want from your other farms.

**Edit an Application**

You can use the following procedure to edit an application.

**Procedure**

1 Select an application on the Applications page and click the **Edit** button at the top of the page.

The Edit Application dialog appears.
2 Edit information as described below.

**Note** Some items are not editable.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Unique name for the application</td>
</tr>
<tr>
<td>Display Name</td>
<td>Name for the application that you want displayed to end users when they see the application in their clients, such as in Horizon Client or the browser using Horizon HTML Access.</td>
</tr>
<tr>
<td>Pod</td>
<td>This option only displays if your data center is configured with multiple pods. Displays the name of the pod where the farm is located.</td>
</tr>
<tr>
<td>Farm</td>
<td>The farm that was specified when the application was added into your inventory.</td>
</tr>
<tr>
<td>Application Path</td>
<td>Location of the application executable on the VM (for example, Z:\Customapps\app.exe) or UNC-specified path (for example, \fileserver.accounting.com\vol1\software\app.exe )</td>
</tr>
<tr>
<td>Icon File</td>
<td>.png file (32 x 32 pixels) to use as application’s icon. [optional] Click Choose File to browse for file.</td>
</tr>
<tr>
<td>Application available on Farm</td>
<td>This option reflects the choice that was specified when the application was added into your inventory.</td>
</tr>
<tr>
<td>Version</td>
<td>Version number of application [optional]</td>
</tr>
<tr>
<td>Publisher</td>
<td>Publisher of application [optional]</td>
</tr>
<tr>
<td>Start Folder</td>
<td>Specify the location in the RDS server VM's Windows operating system that you want the remote application to use as its start folder. <strong>Note</strong> If you specify a LNK file in the Application Path that specifies its own start directory, the system does not use the location specified here.</td>
</tr>
<tr>
<td>Parameters</td>
<td>Specify any command line parameters you want used when the remote application is launched.</td>
</tr>
</tbody>
</table>

3 Click **Save**.

**Delete an Application**

You can use the following procedure to delete an application

**Procedure**

1 Select an application on the Applications page and click the Delete button at the top of the page.  
   The confirmation dialog appears.

2 Click **OK** to confirm delete.

**Rename an Application**

You can use the following procedure to rename an application.
Procedure

1. On the Applications page, select an application and click the **Rename** button at the top of the page.
   
   The Rename dialog appears.

2. Enter the new name and click **Save**.
   
   The new application name appears in the list.

Hide an Application

You can use the following procedure to hide (disable) an application on the Applications page.

**Note** This does not delete the application from the system, but only disables it. The application is moved from the list of visible (enabled) to the list of hidden (disabled) applications. To delete an application, use the Delete function.

Procedure

1. Select an application on the Applications page.

2. Click the **Hide** button at the top of the page.

   The application is disabled and is moved to the hidden applications list.

Unhide an Application

You can use the following procedure to unhide (re-enable) an application on the Applications page.

Procedure

1. Select Hidden in the Show filter at the top of the Applications list.

   The view switches from a list of visible (enabled) to a list of hidden (disabled) applications.

2. Select the application and click **Unhide**.

   The application is re-enabled and moved to the visible (enabled) applications list.

Import Applications Using App Volumes

VMware App Volumes™ is an integrated and unified application delivery and end-user management system for Horizon® and virtual environments. You can use the AppCapture component of App Volumes to create AppStacks for provisioning applications to users.

**Note** the following:

- App Volumes integration must be enabled for you by your VMware representative before you can use this feature.

- App Volumes is not supported for Dedicated Desktops - Traditional Clone assignments. App Volumes can be used with Instant Clone assignments only.
There are three steps in this process:

- Create an AppStack using AppCapture.
- Copy the AppStack into an application file share.
- Import the AppStack into Horizon Cloud.

The first two steps above are performed on a separate computer--that is, outside of the user interface.

Create an AppStack Using AppCapture

Use the AppCapture tool to create an AppStack on a separately-managed computer that contains the applications you wish to capture for assignments.

- To create an AppStack using AppCapture, follow the procedure in Managing Applications for Deployment with AppCapture.
- When you have finished creating the AppStack, copy it to the file share. See Copy an AppStack to a File Share

Managing Applications for Deployment with AppCapture

You use AppCapture to create AppStacks for provisioning applications to user groups.

Before you can assign applications to users, you must capture and package applications into AppStacks by using the AppCapture utility. You then manually copy the AppStacks to a file share.

AppCapture System Requirements

Review these AppCapture minimum requirements for Windows platforms.

AppCapture System Requirements

To install and run AppCapture, verify that your system meets the following minimum requirements.

- OS: AppCapture works on Windows 7 and Windows 10 platforms, for both x86 (32-bit) and 64-bit machines: physical, Workstation, or ESX VMs.
- Disk space: The amount of disk space required depends on the number and size of the applications that you are provisioning. Verify that your system has enough disk space for all the AppStacks that you are creating.
- AppCapture Client: To use the AppCapture Client that is installed with AppCapture, you must have .Net 4.6.1 installed on your system.

Install AppCapture

Use the AppCapture utility to package applications to copy to a file share.

Prerequisites

Ensure that you do not have the App Volumes agent installed on the virtual machine where you plan to install AppCapture. If you have the App Volumes agent installed on the machine, take a snapshot of the machine, clone it, and uninstall the agent.

Procedure

1. Log in as administrator to the machine where you want to install AppCapture.
2. Download the AppCapture installer, VMware-appvolumes-appcapture-<buildnumber>.exe from the VMware downloads page.
3. Double-click the installer and follow the on-screen instructions to install AppCapture.
4. Wait for the machine to reboot and verify that AppCapture.exe is installed under C:\Program Files(x86)\VMware\AppCapture.

What to do next

- The UEM Application profiler is also installed with the AppCapture utility. You can personalize AppStacks using the UEM Application profiler.
- When you install AppCapture, the AppCapture GUI is also installed on your system. Use the AppCapture Client to create and manage App Bundles. See Using the AppCapture Client.

Using AppCapture

Before you can assign applications to users, you must package the applications into AppStacks. An AppStack is a collection of files, folders, registries, and metadata stored in .vhd or .vmdk files. The AppStack is accompanied by a .json file.

You use AppCapture to create and manage AppStacks. AppCapture is a standalone utility which you run outside of App Volumes. You can run AppCapture from a command line, from the AppCapture GUI, or using Microsoft PowerShell.

You create AppStacks on a virtual machine with the AppCapture utility.

App Volumes uses only .vmdk files. You might use .vhd files to install applications on a physical machine with other VMware products.

AppCapture and UEM Application Profiler

You might want to personalize an AppStack after capturing the applications in it, without performing an actual assignment.

You can use the UEM application profiler that is packaged with the AppCapture installer for personalization. When you use the AppCapture.exe command with the /personalize option, the UEM application profiler window is displayed. You can choose the applications you want to personalize and store the settings.

See AppCapture Command-Line Options for details about using the /personalize option.
## Run AppCapture from the Command Line

You can run AppCapture from a command line.

**Note**  You must capture applications from the same operating system into which you mount them. For example, if users are operating a Win7x64 operating system, you must capture the applications by using a similar or an identical base operating system Win7x64 image.

### Prerequisites

1. You must run AppCapture as administrator.
2. Verify that User Account Control (UAC) in Windows is disabled. To turn off UAC, see [http://windows.microsoft.com/en-us/windows/turn-user-account-control-on-off#1TC=windows-7](http://windows.microsoft.com/en-us/windows/turn-user-account-control-on-off#1TC=windows-7).
3. Verify that the CLI command `AppCapture.exe` is installed in `C:\Program Files (x86)\VMware\AppCapture` (64-bit machines) or `C:\Program Files\VMware\AppCapture` (32-bit machines).
4. To view options of the `AppCapture.exe` command, see [AppCapture Command-Line Options](#).

### Procedure

1. Take a snapshot of the system.
   
   You can revert to the snapshot after the capture session.
2. Open a console window.
3. Run the `AppCapture.exe` command: `AppCapture.exe /n your_appstack_name`.
   
   Do not press Enter at this point.

   The AppStack virtual machine disk is usually ready in less than a minute.
4. Minimize the AppCapture console window and run the regular Windows installation to capture each of the application installers.
   
   a. Accept the default installation of all applications on the C: drive. The installation activity redirects to the virtual output disk.
   
   b. If an installer requires a reboot, wait for the reboot to finish.
   
   c. If this feature is available, you can also run ThinApp MSI packages. You can install these packages in the same way that you install other application MSI packages. See the latest ThinApp documentation for information about how to create ThinApp MSI packages.
5  Finish virtual disk creation.
   a  After all installers that are required to be captured in this AppStack have run, return to the console window.
   b  Press Enter to initiate a reboot and finish virtual disk creation.
      After the reboot, you see new AppStacks containing applications.
   c  Verify that you have new VHD and VMDK files in
      C:\ProgramData\VMware\AppCapture\appvhd.

6  Run the AppCapture.exe command to view applications in the VHD file and VMDK files. For VHD files:
   AppCapture.exe /list my_AppStack_Name.vhd and for VMDK files:
   AppCapture.exe /list my_AppStack_Name.vmdk

7  Copy the AppStacks that you have created to a staging file share of your choice.

8  Revert to the system snapshot that you captured before you started the first capture session.

9  Copy the AppStacks from the staging file share to your system.

**AppCapture Command-Line Options**

Use the AppCapture command-line options to create and manage AppStacks.

AppCapture.exe Command Options

The /meta, /vhd, and /vmdk options are useful if you accidentally delete a JSON, VHD, or VMDK file. If a JSON file is deleted, App Volumes cannot read the AppStack.

You can personalize an AppStack using the /personalize command.

The AppCapture.exe command accepts the following options:

**Table 7-1. AppCapture.exe Command-line Options**

<table>
<thead>
<tr>
<th>Task</th>
<th>Option</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display help for the AppCapture.exe command.</td>
<td>/?</td>
</tr>
<tr>
<td>Specify an author's name for the AppStack.</td>
<td>/a</td>
</tr>
<tr>
<td>If the name contains at least one space, put</td>
<td></td>
</tr>
<tr>
<td>the name in parentheses.</td>
<td></td>
</tr>
<tr>
<td>Example: AppCapture.exe /n/a (IT Admin)</td>
<td></td>
</tr>
<tr>
<td>Specify a description for an AppStack.</td>
<td>/d</td>
</tr>
<tr>
<td>Example: This disk contains XYZ suite of</td>
<td></td>
</tr>
<tr>
<td>applications.</td>
<td></td>
</tr>
<tr>
<td>List the contents of the AppStack JSON, VHD,</td>
<td>/list</td>
</tr>
<tr>
<td>and VMDK files. If you are not using the</td>
<td></td>
</tr>
<tr>
<td>default directory, specify the directory</td>
<td></td>
</tr>
<tr>
<td>where the files are located.</td>
<td></td>
</tr>
<tr>
<td>Example: AppCapture.exe /list filePath</td>
<td></td>
</tr>
<tr>
<td>Generate a .json file by using a VMDK file as</td>
<td>/meta</td>
</tr>
<tr>
<td>input. If you are not using the default path,</td>
<td></td>
</tr>
<tr>
<td>specify the path containing the VMDK file.</td>
<td></td>
</tr>
<tr>
<td>Example: AppCapture.exe /meta appStackPath.</td>
<td></td>
</tr>
<tr>
<td>Create an AppStack.</td>
<td>/n</td>
</tr>
<tr>
<td>Example: AppCapture.exe /n</td>
<td></td>
</tr>
<tr>
<td>Task</td>
<td>Option</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>---------------</td>
</tr>
<tr>
<td>Specify an output directory for the AppStack files. The default</td>
<td>/o</td>
</tr>
<tr>
<td>directory is C:\ProgramData\VMware\AppCapture\appvhds.</td>
<td></td>
</tr>
<tr>
<td>You can use this option with the /s option to create an AppStack</td>
<td></td>
</tr>
<tr>
<td>from an existing AppStack. See Update an AppStack from the</td>
<td></td>
</tr>
<tr>
<td>Command Line.</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>AppCapture.exe /s oldAppStackDir /o newAppStackDir</td>
<td></td>
</tr>
<tr>
<td>Specify a source directory for the AppStack files. The default</td>
<td>/s</td>
</tr>
<tr>
<td>directory is C:\ProgramData\VMware\AppCapture\appvhds.</td>
<td></td>
</tr>
<tr>
<td>Do not use this option if you are installing a new application.</td>
<td></td>
</tr>
<tr>
<td>You can use this option with the /o option to create an AppStack</td>
<td></td>
</tr>
<tr>
<td>from an existing AppStack. See Update an AppStack from the</td>
<td></td>
</tr>
<tr>
<td>Command Line.</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>AppCapture.exe /s oldAppStackDir /o newAppStackDir</td>
<td></td>
</tr>
<tr>
<td>You can also use the /s option with /n to update an old AppStack</td>
<td></td>
</tr>
<tr>
<td>with a new one. In this example, the existing oldAppStack.vhd</td>
<td></td>
</tr>
<tr>
<td>AppStack is copied as a base AppStack and can be updated as</td>
<td></td>
</tr>
<tr>
<td>newAppstackName:</td>
<td></td>
</tr>
<tr>
<td>AppCapture.exe /n newAppstackName /s oldAppStack.vhd /o newAppStackDir</td>
<td></td>
</tr>
<tr>
<td>Create a .vhd file from a .vmdk file. If you are not using the</td>
<td>/vhd</td>
</tr>
<tr>
<td>default path, specify the path containing the .vhd file.</td>
<td></td>
</tr>
<tr>
<td>Example: AppCapture.exe /vhd appStackPath.vmdk</td>
<td></td>
</tr>
<tr>
<td>Generate a VMDK file by using a VHD file as input. If you are not</td>
<td>/vmdk</td>
</tr>
<tr>
<td>using the default path, specify the path containing the .vhd file.</td>
<td></td>
</tr>
<tr>
<td>Example: AppCapture.exe /vmdk appStackPath.vhd.</td>
<td></td>
</tr>
<tr>
<td>Task</td>
<td>Option</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Virtualize the application after provisioning it for pre-verification. When using the /test option with no other parameters, the AppStack should contain only one application bundle.</td>
<td>/test &lt;Provisioned AppStackPath&gt;.vhd [*</td>
</tr>
<tr>
<td>Example: AppCapture.exe /test Provisioned appStackPath.vhd</td>
<td></td>
</tr>
<tr>
<td>Virtualize all application bundles in the AppStack. Example:</td>
<td></td>
</tr>
<tr>
<td>AppCapture.exe /test Provisioned appStackPath.vhd *</td>
<td></td>
</tr>
<tr>
<td>Virtualize application bundles that are identified by their corresponding GUIDs in the AppStack. Example:</td>
<td></td>
</tr>
<tr>
<td>AppCapture.exe /test Provisioned appStackPath.vhd GUID1, GUID2.. GUIDn</td>
<td></td>
</tr>
<tr>
<td>Enable the user to personalize the application bundle using the UEM application profiler. Configuration files that contain the personalization settings are generated. By default, the files are saved in the same location as the VHD, under the UEMConfigFiles\AppStack folder.</td>
<td>/personalize &lt;ProvisionedAppStackPath&gt;.vhd [/predef</td>
</tr>
<tr>
<td>Example: AppCapture.exe /personalize C:\FinanceApps.vhd -</td>
<td></td>
</tr>
<tr>
<td>Personalization settings are saved under</td>
<td></td>
</tr>
<tr>
<td>C:\ProgramData\VMware\AppCapture\appvhds\UEMConfigFiles\FinanceApps</td>
<td></td>
</tr>
<tr>
<td>The /predef sub-option is an optional boolean switch that can be used with the /personalize option to capture the predefined settings of the specified application bundle into a configuration file. The predefined settings are captured in an additional configuration file.</td>
<td></td>
</tr>
<tr>
<td>Example: AppCapture.exe /personalize C:\FinanceApps.vhd /predef -</td>
<td></td>
</tr>
<tr>
<td>Personalization settings along with predefined settings are saved under</td>
<td></td>
</tr>
<tr>
<td>C:\ProgramData\VMware\AppCapture\appvhds\UEMConfigFiles\FinanceApps</td>
<td></td>
</tr>
<tr>
<td>The /flexconfigname sub-option can be used with the /personalize command to store the personalization settings into a user-friendly configuration file name.</td>
<td></td>
</tr>
<tr>
<td>Example: AppCapture.exe /personalize</td>
<td></td>
</tr>
<tr>
<td>C:\FinanceApps.vhd /flexconfigname MSOffice2016 -</td>
<td></td>
</tr>
<tr>
<td>Personalization settings are saved under</td>
<td></td>
</tr>
<tr>
<td>C:\ProgramData\VMware\AppCapture\appvhds\UEMConfigFiles\MSOffice2016</td>
<td></td>
</tr>
</tbody>
</table>

**Merging AppStacks**

You can merge two or more AppStacks from the command line by using AppMerge.
Use AppMerge to merge two or more existing AppStacks into one file. AppMerge takes as its input VHD files associated with an AppStack.

**Note**  The input AppStack files must all be of type VHD. You can create a merged output AppStack of a different type with the /vhd and /vmdk options.

AppMerge has this syntax:

```
AppMerge.exe /o outputAppStack /s "inputAppStack1file","inputAppStack2file", "inputAppStack3file",...
```

Example: **Creating a Merged AppStack**

In this example, you create an AppStack file called MergedAppstack.vhd from three existing AppStack files, Office.vhd, Notepad++.vhd, and Firefox.vhd:

```
AppMerge.exe /o C:\MergedAppstack.vhd /s "Office.vhd","Notepad++.vhd","Firefox.vhd"
```

You can specify input file paths, output file paths, and file names. In this case, the three input AppStacks are presumed to be in the default AppStack location. The output AppStack goes in the C: drive.

Besides the /o and /s parameters, AppMerge accepts the following options:

- /df. Deletes a specific application bundle. Takes a full path of a file that contains a single GUID in each line as its arguments.
- /dl. Deletes a specific application bundle. Takes comma-separated GUIDs as arguments.
- /list. Lists the content of the newly created AppStack file.
- /vhd. Creates a VHD output AppStack file from VMDK AppStack input files.
- /vmdk. Creates a VMDK output AppStack file from VHD AppStack input files.

See also **AppCapture Command-Line Options**.

**Update an AppStack from the Command Line**

You update an AppStack to add applications, update existing applications, or remove applications from the AppStack.

**Prerequisites**

Verify that you have the correct credentials and you are taking the appropriate precautions:

- Run AppCapture as administrator.
- Create at least one AppStack.
- Become familiar with the command options that apply to updating an AppStack. See **AppCapture Command-Line Options**.)
Procedure

1. Open the command prompt and navigate to the AppCapture folder with either `cd "\Program Files\VMware\AppCapture"` (64-bit) or `cd "\Program Files (x86)\VMware\AppCapture"` (32-bit).

2. Update an AppStack:
   a. Run `AppCapture.exe /n appStackName /s sourceAppStackDir`.
      
      `sourceAppStackDir` is the path of the AppStack that you want to update.
      
      This example takes an existing AppStack and updates it into a new update AppStack:
      ```
      AppCapture.exe /n AdminUser2.0 /s "C:ProgramData\VMware\AppCapture\appvhds\AdminUser1.0" /o C:\NewFolder
      ```
      
      You can include other command options that apply to updating an AppStack.
      
      The AppStack is created and stored in the location that you specify, or by default in the appvhds folder.
   b. Add applications, update existing applications, or remove applications from the AppStack.

<table>
<thead>
<tr>
<th>Task</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add applications or update existing applications</td>
<td>Run the installers for the applications that you want to install or update on the AppStack.</td>
</tr>
<tr>
<td>(Optional) Remove applications</td>
<td>1. Navigate to Control Panel &gt; Programs and Features.</td>
</tr>
<tr>
<td></td>
<td>2. Select the applications that you want to remove from the AppStack and complete the uninstall procedure.</td>
</tr>
</tbody>
</table>

3. After you add or remove the applications, navigate to the command prompt and press **Enter**.

4. Press **Enter** to restart the machine and finalize the AppStack update procedure.

After the machine restarts, the JSON, VHD, and VMDK files are created. When the application capture process finishes, the applications are removed from the machine.

**Using AppCapture with Microsoft PowerShell**

You can use Microsoft PowerShell cmdlets to capture applications, create and update AppStacks, and recreate deleted AppStacks with AppCapture. You can use the 32-bit or 64-bit PowerShell console to run the AppCapture module.

You can also run AppCapture from the command line, as described in Run AppCapture from the Command Line.

**Note** You must capture applications from the same OS into which you mount them. For example, if users are operating a Win7x64 OS, you must capture the applications by using a similar or an identical base OS Win7x64 image.
Run AppCapture Using PowerShell

You can run AppCapture using Microsoft PowerShell.

Prerequisites

Verify that you are logged in as administrator and you are taking the appropriate precautions:

- Run AppCapture as administrator.
- Become familiar with the AppCapture cmdlets. See PowerShell Options and Parameters

Procedure

1. Take a snapshot of the system.
   You can revert to the snapshot after the capture session.
2. Open a 32-bit or 64-bit PowerShell console,
3. Import the PowerCLI module using the `import-module vmware.appcapture` command.
   This imports the AppCapture module.
4. (optional) To see a list of all modules, run the `get-module` command.
5. Run the command `Start-AVAppCapture -Name appStackFile`, where `appStackFile` is the name of the AppStack .vhd file to create.
   Do not press Enter yet.
   `appStackFile`.vhd is created.
6. Leave the PowerShell console and install, on this machine, any applications to be provisioned.
7. After all of the applications have been installed, open the PowerShell console again.
8. Press Enter.
9. Reboot your machine if necessary.
   In the AppCapture console window you see the locations of the AppStack files .json, .vhd and .vmdk. By default, these files are stored in C:\ProgramData\VMware\AppCapture\appvhds.
10. (Optional) Examine the .json, .vhd, and .vmdk files in that directory to ensure that the applications have been bundled.
11. Copy the AppStacks that you have created to a staging file share.
12. Revert to the system snapshot that you captured before you started the first capture session.
13. Copy the AppStacks from the staging file share to your system.

PowerShell Options and Parameters

You can use several options when you run AppCapture with Microsoft PowerShell.

AppCapture Options and Parameters with PowerShell
Use the Start-AVAppCapture to create an AppStack and add applications to it. The UEM Application Profiler is installed with the AppCapture utility and you can personalize the AppStacks using the profiler.

**Table 7-2. Start-AVAppCapture Options**

<table>
<thead>
<tr>
<th>Start-AVAppCapture Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-Author Author-name</td>
<td>Specify an author who is associated with this AppStack.</td>
</tr>
<tr>
<td>CommonParameters</td>
<td>Use one or more common parameters. The common parameters are a set of cmdlet parameters implemented by Windows PowerShell. Start-AVAppCapture supports these common parameters:</td>
</tr>
<tr>
<td></td>
<td>- Debug</td>
</tr>
<tr>
<td></td>
<td>- ErrorAction</td>
</tr>
<tr>
<td></td>
<td>- ErrorVariable</td>
</tr>
<tr>
<td></td>
<td>- OutBuffer</td>
</tr>
<tr>
<td></td>
<td>- OutVariable</td>
</tr>
<tr>
<td></td>
<td>- PipelineVariable</td>
</tr>
<tr>
<td></td>
<td>- Verbose</td>
</tr>
<tr>
<td></td>
<td>- WarningAction</td>
</tr>
<tr>
<td></td>
<td>- WarningVariable</td>
</tr>
<tr>
<td>For more information about common parameters, see about_CommonParameters.</td>
<td></td>
</tr>
<tr>
<td>-Description text</td>
<td>Specify a description for an AppStack. If the description includes a space, enter the description inside parentheses, for example, -Description (HR Apps).</td>
</tr>
<tr>
<td>-Destination output-directory</td>
<td>Specify an output directory for an AppStack. By default, AppStacks are placed in C:\ProgramData\VMware\AppCapture\appvhds.</td>
</tr>
<tr>
<td>-Force</td>
<td>Create an output directory if it does not exist. You specify the output directory with the -Destination parameter.</td>
</tr>
<tr>
<td>-Name vhd-name</td>
<td>Specify a name for the applications being captured. The output .vhd file is named by using the specified application name.</td>
</tr>
<tr>
<td>-Novmdk</td>
<td>Specify this option to prevent post-capture VMDK disk creation.</td>
</tr>
<tr>
<td>-Path directory-path</td>
<td>Specify a path to an AppStack. The AppStack is used as a template for the current capture. Do not use this option if you are installing a new application.</td>
</tr>
</tbody>
</table>

You can perform several workflows with the AppCapture command.

**Table 7-3. AppCapture PowerShell Workflows**

<table>
<thead>
<tr>
<th>Workflow</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ConvertTo-AVVhdDisk</td>
<td>Generate a .vhd file by using the .vmdk file as input.</td>
</tr>
<tr>
<td>ConvertTo-AVVmdkDisk</td>
<td>Generate a .vmdk file by using the .vhd file as input.</td>
</tr>
<tr>
<td>Export-AVMetadata</td>
<td>Generate a .json file by using a .vhd or .vmdk file as input.</td>
</tr>
</tbody>
</table>
### Table 7-3. AppCapture PowerShell Workflows (Continued)

<table>
<thead>
<tr>
<th>Workflow</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Merge-AVAppDisks</td>
<td>Merge AppStack .vhd files into a new AppStack .vhd. Merging AppStacks describes the command-line version, which is similar.</td>
</tr>
<tr>
<td>Remove-AVApp</td>
<td>Delete an AppStack from a disk or remove specific applications from an AppStack. If you remove any applications from the AppStack, the AppStack must be imported again into the App Volumes Manager.</td>
</tr>
<tr>
<td>Reset-AVConfig</td>
<td>Clear AppCapture configuration information from the machine.</td>
</tr>
<tr>
<td>Show-AVDiskDetails</td>
<td>List the contents of the .vhd file, .json file, or .vmdk file.</td>
</tr>
<tr>
<td>Start-AVAppCapture</td>
<td>Start the procedure to capture applications.</td>
</tr>
<tr>
<td>Start-AVAppUpdate</td>
<td>Update an AppStack.</td>
</tr>
<tr>
<td>Test-AVAppStack</td>
<td>Attach or virtualize applications after provisioning the application.</td>
</tr>
<tr>
<td>Start-AVAppPersonalization</td>
<td>Attach the AppStack (.vhd) and personalize the specified application bundle using the UEM Application Profiler.</td>
</tr>
</tbody>
</table>

The examples below include the workflow file paths and the commands to reach the workflows.

- Begin a new capture session. The output is generated in the form of a .vhd file and is named AdobeSuite.vhd. The author is John and a description is added.

  ```powershell
  Start-AVAppCapture -Name AdobeSuite -Author John -Description "This disk contains the AdobeSuite application"
  ```

- ConvertTo-AVVhdDisk. This example generates an output .vhd format file, Adobe.vhd, from a source file, Adobe.vmdk. The output file is placed in a different directory from the source file:

  ```powershell
  ConvertTo-AVVhdDisk -Path "C:\Program Files (x86)\VMware\AppCapture\appvhds\Adobe.vmdk" -Destination "C:\AppCaptures"
  ```

- Export-AVMetadata. This example generates the output metadata file Adobe.json. The file is generated in the same place as Adobe.vhd:

  ```powershell
  Export-AVMetadata -Path "C:\Program Files (x86)\VMware\AppCapture\appvhds\Adobe.vhd"
  ```

- Merge-AVAppDisks. This example merges all the .vhd files under the .\temp and .\appstacks directories and generates a Notepad+Adobe.vhd file in \temp.

  ```powershell
  Merge-AVAppDisks -Path .\temp\*.vhd .\appstacks\*.vhd -Destination c:\temp\Notepad+Adobe.vhd
  ```

- Remove-AVApp. This example deletes the Adobe and Notepad applications from the input disk Adobe+Notepad.vhd. Each application is identified by its unique GUID:

  ```powershell
  Remove-AVApp -Path C:\Temp\Adobe+Notepad.vhd -Destination c:\Temp\empty.vhd -Guids GUID1, GUID2
  ```
Show-AVDiskDetails. This example displays the details from a .json file. The syntax is the same for .vhd and .vmdk files:

```
Show-AVDiskDetails -Path "C:\Program Files (x86)\VMware\WEM Capture\appvhds\Adobe.json"
```

Start-AVAppUpdate. This example updates the AdobeSuite.vhd with a hot fix. A copy of AdobeSuite.vhd is created and is named AdobeHotfixUpdate.vhd. All the hot fix installations are captured in AdobeHotfixUpdate.vhd:

```
Start-AVAppUpdate -Name AdobeHotfixUpdate -Path "C:\Program Files (x86)\VMware\AppCapture\appvhds\AdobeSuite.vhd"
```

Test-AVAppStack -Path. Virtualize the application after provisioning it for pre-verification. When using this command with no other parameters, the AppStack should contain only one application bundle.

```
Test-AVAppStack -Path C:\Program Files (x86)\VMware\WEMCapture\appvhds\Chrome.vhd
```

Test-AVAppStack -Path "C:\Program Files (x86)\VMware\WEMCapture\appvhds\HRApps.vhd" -Guids Guid1Guid2..Guid1..GUIDn. This cmdlet virtualizes application bundles that are identified by their corresponding GUIDs in the AppStack.

```
Test-AVAppStack -Path "C:\Program Files (x86)\VMware\WEMCapture\appvhds\HRApps.vhd" -Guids "*". This cmdlet virtualizes all application bundles in the AppStack.
```

Start-AVAppPersonalization -Path. This cmdlet attaches the VHD and enables the user to personalize the application bundle using the UEM application profiler. Personalization settings are saved in C:\ProgramData\VMware\AppCapture\appvhds\UEMConfigFiles\Chrome.

```
Start-AVAppPersonalization -Path "C:\ProgramData\VMware\AppCapture\appvhds\Chrome.vhd"
```

Start-AVAppPersonalization -Path "C:\appvhds\Chrome.vhd" --Predef. This cmdlet attaches the VHD and enables the user to personalize the application bundle using the UEM application profiler. Predefined settings and personalization settings are saved in C:\ProgramData\VMware\AppCapture\appvhds\UEMConfigFiles\Chrome.

```
Start-AVAppPersonalization -Path "C:\appvhds\Chrome.vhd" --Name Browser1. This cmdlet attaches the VHD and enables the user to personalize the application bundle using the UEM application profiler. Personalization settings files are saved in C:\ProgramData\VMware\AppCapture\appvhds\UEMConfigFiles\Browser1.
```

To get help about the workflows, run the `get-help` command.

**Table 7-4. AppCapture PowerShell Workflow Information and Examples**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>get-help WorkFlowName</td>
<td>View general information for a workflow.</td>
</tr>
<tr>
<td>get-help WorkFlowName -detailed</td>
<td>View detailed information for a workflow.</td>
</tr>
</tbody>
</table>
Table 7-4. AppCapture PowerShell Workflow Information and Examples (Continued)

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>get-help WorkFlowName -examples</td>
<td>View an example of a workflow.</td>
</tr>
<tr>
<td>get-help WorkFlowName -full</td>
<td>View technical information for a workflow.</td>
</tr>
</tbody>
</table>

Using the AppCapture Client

The AppCapture Client consists of a GUI that you can use to simplify the AppCapture process.

Use the AppCapture Client to create, update, merge, and test App Bundles. You can also update merged AppStacks and perform several post-capture actions. AppStacks are named App Bundles in the GUI.

When you enter the AppCapture commands in the GUI, the corresponding command string is automatically generated. You can copy and paste the string to the command-line. Click Show Script to view the generated string.

Add a File Share

You must add a file share before you can work with the AppCapture Client to create and manage App Bundles.

Prerequisites
- It is recommended that the file share you are adding is a remote file share.
- Ensure that the file share is mounted on the machine using domain credentials.

Procedure
1. Start the AppCapture Client and go to Settings > File Share.
2. Browse to the location of the file share and select the file share.
3. Click Add.
   - The Name field is automatically populated.
4. (Optional) Provide a name for the Author.
5. Click Save.
   - You are taken to the App Bundles page.

What to do next

You can now begin to capture, update, and test App Bundles.

Create an App Bundle

Create an App Bundle and capture applications into it using the AppCapture Client.

Note  App Bundles can contain more than one application. However, to take full advantage of the AppToggle and AppMerge features, install only one application in an App Bundle. See Create a Merged App Bundle.
Procedure

1. From the AppCapture Client, click **APP BUNDLES**.

2. Click **Capture** and provide the following information:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name (Required)</td>
<td>The name of the App Bundle.</td>
</tr>
<tr>
<td>Description (Optional)</td>
<td>Description of the App Bundle.</td>
</tr>
<tr>
<td>Author (Optional)</td>
<td>Name of the person who created the App Bundle. Defaults to the current user or the name that is stored in the application's settings.</td>
</tr>
<tr>
<td>Destination (read-only)</td>
<td>Automatically populated with the selected file share location. The App Bundle files, VHD and associated JSON files are created in this location.</td>
</tr>
</tbody>
</table>

   The command script that is generated is shown at the bottom of the screen.

3. Click **Create**.

   The AppCapture process is launched. You are prompted to install the applications you want to capture in the App Bundle. Continue to follow on-screen directions to complete the task of creating the App Bundle.

What to do next

The capture process is completed only after the virtual machine reboots. After the machine has rebooted, and the AppCapture Client has restarted automatically, go to the **APP BUNDLES** page. Double-click the bundle you created and verify that the bundle contains the applications you installed in it.

Update an App Bundle

You can use the AppCapture Client to edit and update the information in an App Bundle and install new applications in the bundle.

**Note** An App Bundle can contain more than one application. However, to take full advantage of the AppToggle and AppMerge utilities, install only one application in an App Bundle.

Procedure

1. From the AppCapture Client, click **APP BUNDLES**.

2. Select the bundle that you want to update.

3. Click **Update** and edit the required information:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>New Name (Required)</td>
<td>The new name of the App Bundle. Must be different from the existing name.</td>
</tr>
<tr>
<td>Description (Optional)</td>
<td>Description of the App Bundle.</td>
</tr>
</tbody>
</table>
Create a Merged App Bundle

You can merge two or more single App Bundles to create a merged App Bundle.

**Note**  To take full advantage of the AppToggle facility, you can only merge single App Bundles into an AppStack. You cannot merge an already merged App Bundle with another App Bundle.

**Procedure**

1. From the AppCapture Client, click **MERGED APP BUNDLES**.
2. Provide the following information.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name (Required)</td>
<td>The name of the bundle.</td>
</tr>
<tr>
<td>Description</td>
<td>Description of the bundle.</td>
</tr>
<tr>
<td>Author</td>
<td>Name of person or entity who created the merged bundle. Defaults to the current user or the name that is stored in the application's settings.</td>
</tr>
<tr>
<td>Destination</td>
<td>Location where the merged bundle is to be saved.</td>
</tr>
</tbody>
</table>

3. Click **Add**.

A list of App Bundles that can be merged is displayed.

4. Select the bundles and click **OK**.

5. Click **Create**.

A message is displayed after the merge operation is complete. Click the log to view the details of the merge operation.

**Update a Merged App Bundle**

You can update a merged bundle to add or delete applications.

**Prerequisites**

You must have created a merged App Bundle before you can update the bundle. See [Create a Merged App Bundle](#).
**Procedure**

1. From the AppCapture Client, click **Merged App Bundles**.
2. Select a merged bundle and click **Update**.
   
The list of bundles contained in the merged bundle is displayed.
3. Edit the required information:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>New Name (Required)</td>
<td>The new name of the merged App Bundle. Must be different from the existing name.</td>
</tr>
<tr>
<td>Description (Optional)</td>
<td>Description of the App Bundle.</td>
</tr>
<tr>
<td>Author (Optional)</td>
<td>Name of the person who created the App Bundle. Defaults to the current user or the name that is stored in the application's settings.</td>
</tr>
<tr>
<td>Destination (read-only)</td>
<td>Automatically populated with the location of the App Bundle you want to update. This is the same as the selected file share location.</td>
</tr>
</tbody>
</table>

   The command script that is generated is shown at the bottom of the screen.
4. Click **Edit** and select the application(s) you want to add or remove.
   
The list of applications captured in the bundle is displayed.
5. Click **OK**.
6. Review the updated contents of the bundle and click **Update**.
7. Click **Yes** to confirm that you want to update the merged bundle.

**Test an App Bundle**

Use the AppCapture Client to verify if applications have been captured successfully in an App Bundle and if the bundle works as expected.

**Prerequisites**

Take a snapshot of the machine before running the **Test** command. You must have captured applications in an App Bundle before you can test it.

**Procedure**

1. From the AppCapture Client, click one of the following:
   - **App Bundles** to test a single App Bundle.
   - **Merged App Bundles** to test a merged App Bundle.
2. Select a bundle from the list and click **Test**.
   
The selected bundle is mounted and App Volumes verifies the bundle.

**AppCapture Folders and Files**

AppCapture creates several files and folders.

AppCapture creates various folders in `C:\ProgramData\VMware\AppCapture\appvhds`. 
Table 7-5. AppCapture Folders

<table>
<thead>
<tr>
<th>Folder</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>appvhds</td>
<td>.vhd, .json, and .vdmk files that are generated when you create an AppStack by using AppCapture.</td>
</tr>
<tr>
<td>logs</td>
<td>Log file generated by AppCapture. The log file is named AppCapture.log and is located in C:\ProgramData\VMware\AppCapture\logs.</td>
</tr>
<tr>
<td>modules</td>
<td>PowerCLI .dll files that are required to perform PowerCLI operations.</td>
</tr>
<tr>
<td>plugins</td>
<td>VMware Horizon Air plug-ins. Plug-ins convert the AppStack to the correct format for deployment to end users.</td>
</tr>
<tr>
<td>templates</td>
<td>.vhd file templates that act as boilerplate .vhd files on which AppStacks are created.</td>
</tr>
</tbody>
</table>

AppCapture creates these files in the appvhds directory unless you specify a different directory. See AppCapture Command-Line Options.

Table 7-6. AppCapture Files

<table>
<thead>
<tr>
<th>File</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>application.vhd</td>
<td>.vhd file that holds the application files that are part of the AppStack.</td>
</tr>
<tr>
<td>application.vmdk</td>
<td>VMDK-format Virtual Hard Disk file that VMware Horizon Air natively uses.</td>
</tr>
<tr>
<td>application.json</td>
<td>The .json file with information about the applications that are captured in the AppStack.</td>
</tr>
</tbody>
</table>

Copy an AppStack to a File Share

After you have created your AppStack, you must place it in a file share.

Prerequisites

You must first create a file share and add it on the Infrastructure page as an application file share.

Procedure

1. Open a File Explorer window for \share IP\sharename where sharename is the name of your application file share.

2. Copy your AppStack .vmdk and .json files to this directory.

   AppCapture produces two types of files:
   - .vmdk files for mounting AppStacks on virtual machines
   - .vhd files for mounting them on physical machines

   Horizon Cloud uses only .vmdk files. However, you might use .vhd files to install applications on a physical machine with other VMware products.
What to do next

After adding the AppStack to the file share, you must import it. See Import an AppStack into Horizon Cloud.

Import an AppStack into Horizon Cloud

After you have placed an AppStack in an application file share, you can import it into Horizon Cloud.

Procedure

1. Navigate to Settings > Infrastructure.
2. Click File Share.
3. Select the check box for the file share that has the AppStack to import.
   You can import from only one file share at a time.
4. Click ... and select Import.

Troubleshooting App Volumes Functionality

You can use Python scripts to troubleshoot App Volumes functionality.

The scripts described below require Python 2.7.9 or higher.

- Retrieve Mapping Details for Application Assignments

  The script below retrieves details for assignments in your environment.

  **Usage:**

  ```
  xmp_host xmp_domain xmp_user xmp_password
  ```

  **Positional Arguments:**

  - `xmp_host`: XMP host url
  - `xmp_domain`: XMP user domain
  - `xmp_user`: XMP user name
  - `xmp_password`: XMP user password

  **Optional Arguments:**

  - `--help`: show this help message and exit
  - `-t TYPE, --type TYPE All, AppVolumes, DaaS`
  - `-p XMP_PORT, --port XMP_PORT XMP host port`
  - `-o CSV_PATH, --output CSV_PATH Output csv file path`
  - `-u SEARCH_USER, --user SEARCH_USER Search user name`
Script format:

```
mapping_details.py <IP/FQDN> <domain> <username> 'password' -p 8443
```

Code Example (retrieves all assignments):

```
qbi@qbi-vm ~ # mapping_details.py qbi-ubuntu.eng.vmware.com falcon administrator 'password' -p 8443
Get assignments successfully.
qbi@qbi-vm ~ # cat assignments.csv
key,user name,assignment,application name,bundle name,package name,assignment type,Os type
MIRAGEDOMAIN\qbi only||Mozilla Firefox (3.0.3),MIRAGEDOMAIN\qbi only,qbi-only-win10-x64,Mozilla Firefox (3.0.3),Native,Windows 10 (x64)  
MIRAGEDOMAIN\qbi only||Adobe Flash Player 21 NPAPI,MIRAGEDOMAIN\qbi only,qbi-only-win10-x64,Adobe Flash Player 21 NPAPI,,Native,Windows 10 (x64)  
MIRAGEDOMAIN\qbi only||Mozilla Maintenance Service,MIRAGEDOMAIN\qbi only,qbi-only-win10-x64,Mozilla Maintenance Service,,Native,Windows 10 (x64)  
MIRAGEDOMAIN\qbi only||Mozilla Firefox 45.0.1 (x86 en-US),MIRAGEDOMAIN\qbi only,qbi-only-win10-x64,Mozilla Firefox 45.0.1 (x86 en-US),,Native,Windows 10 (x64)  
MIRAGEDOMAIN\qbi only||Python 2.6.6,MIRAGEDOMAIN\qbi only,qbi-only-win10-x64,Python 2.6.6,,Native,Windows 10 (x64)  
FALCON\qbi||Adobe Flash Player 21 NPAPI,FALCON\qbi,qbi-win10-x64,Adobe Flash Player 21 NPAPI,,Native,Windows 10 (x64)  
FALCON\qbi||Mozilla Maintenance Service,FALCON\qbi,qbi-win10-x64,Mozilla Maintenance Service,,Native,Windows 10 (x64)  
FALCON\qbi||Mozilla Firefox 45.0.1 (x86 en-US),FALCON\qbi,qbi-win10-x64,Mozilla Firefox 45.0.1 (x86 en-US),,Native,Windows 10 (x64)  
MIRAGEDOMAIN\qbi||Adobe Flash Player 21 NPAPI,MIRAGEDOMAIN\qbi,qbi-win10-x64,Adobe Flash Player 21 NPAPI,,Native,Windows 10 (x64)  
MIRAGEDOMAIN\qbi||Mozilla Maintenance Service,MIRAGEDOMAIN\qbi,qbi-win10-x64,Mozilla Maintenance Service,,Native,Windows 10 (x64)  
MIRAGEDOMAIN\qbi||Mozilla Firefox 45.0.1 (x86 en-US),MIRAGEDOMAIN\qbi,qbi-win10-x64,Mozilla Firefox 45.0.1 (x86 en-US),,Native,Windows 10 (x64)  
FALCON\Users||FirefoxWin10x64,FALCON\Users,app-bundle-assignment,Mozilla Firefox (3.0.3),FirefoxWin10x64,,Native,Windows 10 (x64)  
FALCON\Users||CutePDF Professional 3.7 (Evaluation),FALCON\Users,users-win7,CutePDF Professional 3.7 (Evaluation),,Native,Windows 7 (x64)  
FALCON\Users||FileZilla Client 3.9.0.6,FALCON\Users,users-win7,FileZilla Client 3.9.0.6,,Native,Windows 7 (x64)  
MIRAGEDOMAIN\Users||CutePDF Professional 3.7 (Evaluation),MIRAGEDOMAIN\Users,users-win7,CutePDF Professional 3.7 (Evaluation),,Native,Windows 7 (x64)  
MIRAGEDOMAIN\Users||FileZilla Client 3.9.0.6,MIRAGEDOMAIN\Users,users-win7,FileZilla Client 3.9.0.6,,Native,Windows 7 (x64)  
```

Retrieve Details for Attach and Detach Failures
The script below retrieves details for attach and detatch failures, including those involving AppStacks.

- **Usage:**

```
usage: fetch_volume_failures.py [-h] [-t SEARCH_DURATION] [-u SEARCH_USER]
                                 [-d SEARCH_DOMAIN] [-s PAGE_SIZE]
                                 [-c | -v | -o CSV_PATH]
                                login_host login_domain login_user
                                login_password
```

- **Positional arguments:**

  - `login_host` Login host url in format hostname:<port>
  - `login_domain` Login user domain
  - `login_user` Login user name
  - `login_password` Login user password

- **Optional arguments:**

  - `-h, --help` show this help message and exit
  - `-t SEARCH_DURATION, --time SEARCH_DURATION` Last1Hour, Last12Hour, Last24Hour, Last72Hour, All
  - `-u SEARCH_USER, --user SEARCH_USER` Search user name
  - `-d SEARCH_DOMAIN, --domain SEARCH_DOMAIN` Search domain name
  - `-s PAGE_SIZE, --size PAGE_SIZE` Size of each page of the results
  - `-c, --concise` Print results in concise view
  - `-v, --verbose` Print results in itemed view
  - `-o CSV_PATH, --output CSV_PATH` Output to csv file in given path (default)

- **Script format:**

  `python fetch_volume_failures.py <IP/FQDN> <domain> <username> ’<password>’`

- **Code Examples:**

  ```
  python fetch_volume_failures.py 10.111.24.65 falcon administrator ’<password>’ # output as volume_failures.csv for last 1 hour
  python fetch_volume_failures.py 10.111.24.65 falcon administrator ’<password>’ -v # show results of last 1 hour in screen
  python fetch_volume_failures.py 10.111.24.65 falcon administrator ’<password>’ -t Last24Hour # show last 24 hour result
  python fetch_volume_failures.py 10.111.24.65 falcon administrator ’<password>’ -t All -u hez -d vmwarem # show all results of hez@vmwarem for last 1 hour
  ```

Each failure record includes the following information:

- **Timestamp**
- **Writable?** - Indicates whether this is a writable volume (Y) or AppStack (N).

  **Note**  Writable Volumes is a Beta feature. Please contact your VMware representative for more information.

- **Attach/Detach** - Indicates whether this is an attach failure or a detach failure.
- **User/domain** - Username and domain for which the failure occurred.
- **File location** - File location. Format is `<datacenter>/<node>/<vcenter>/<datastore>/<vmdk path>`
- **VM Location** - File location. Format is `<datacenter>/<node>/<vcenter>/<vm name>`

When you see attach/detach failures, it is recommended that you check on the following:

- Is the user a member of the appropriate group?
- Is the agent on the desktop installed and up-to-date?

You can also record the failure information for inclusion with a support request.

**Note**  You will also see notifications in the user interface that include basic information for these failures (i.e. number of failures and number of users affected). For more information on notifications, see **Notifications Page**.
Images are patterns that you use to create assignments.

**About Images**

Images are created from template VMs that are configured for the needs of various types of users. You can:

- Receive a pre-packaged image from VMware.
- Create an image from a template you receive from VMware.
- Create an image from your own template.

**Image Types**

There are two types of images, as described below.

<table>
<thead>
<tr>
<th>Image Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Instant Clone</td>
<td>Image type that uses VMware’s NGVC technology to create VMs instantly for an assignment.</td>
</tr>
<tr>
<td>Traditional Clone</td>
<td>Proprietary image type that does full image cloning when creating assignments</td>
</tr>
</tbody>
</table>

The image type is selected when the image is first created.

**The Images Page**

To view images currently in your system, select **Inventory > Images** to display the Images page.

This chapter includes the following topics:

- Managing Images
- Create an Image
- Update Agent Software for an Image
- Build Your Own Template

**Managing Images**

The Images page lists all images currently in the system. The actions you can perform on this page are described below.
There are two ways to perform actions on images.

- Select the check box for an image in the list and use the buttons and menu selections at the top of the page as described below.
- Click on an image to view the image detail page and use the buttons and menu selections at the top of that page. Only some of the options below are available on the image detail page, and they appear in different order.

The image detail page also has options to perform a rollback or delete a backup. See Backup Now below for more information.

You can perform the following actions using buttons at the top of the Images page.

<table>
<thead>
<tr>
<th>Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>New</td>
<td>Begin the image creation process. See Create an Image.</td>
</tr>
<tr>
<td>Rename</td>
<td>Renames the selected image.</td>
</tr>
<tr>
<td>Duplicate</td>
<td>[Instant Clone images only] Creates a duplicate of the selected image.</td>
</tr>
<tr>
<td>Update Agent</td>
<td>Updates agent(s) for a selected image. See Update Agent Software for an Image.</td>
</tr>
</tbody>
</table>

You can perform the following actions by clicking the "..." button at the top of the Images page and making a selection from the drop-down menu.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Backup Now</td>
<td>[Traditional Clone images only] Creates a backup of the selected image.</td>
</tr>
<tr>
<td></td>
<td>After you create and name the backup, it appears under Backups on the image detail page.</td>
</tr>
<tr>
<td></td>
<td>Next to each backup shown on the image detail page there are options to roll back to that backup or to delete it from your system.</td>
</tr>
</tbody>
</table>

**Note** If a backup that was previously listed on the image detail page does not appear, and you have not deleted it, contact your VMware representative to remedy this issue.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Delete</td>
<td>Permanently deletes the selected image.</td>
</tr>
<tr>
<td>Publish</td>
<td>Publishes the selected image.</td>
</tr>
<tr>
<td>Take Offline</td>
<td>Takes the selected image offline. The image cannot be used to make new assignments or to provision new desktops or servers for existing assignments. If you take an image offline, you must republish it to make it available for assignments.</td>
</tr>
<tr>
<td>Convert to Desktop</td>
<td>Converts the selected image to a desktop.</td>
</tr>
<tr>
<td>Assign Image</td>
<td>[Instant Clone images only] Pushes updates to dedicated desktop and floating desktop assignments using the selected image. Select the assignment(s) from the list and click OK to push the updates.</td>
</tr>
<tr>
<td>Launch Console</td>
<td>Launches a console for the VM associated with the selected image. This option is disabled if the VM is powered off or if more than one image is selected.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Push Updates</td>
<td>Pushes updates to assignments using the selected image.</td>
</tr>
<tr>
<td></td>
<td>- Desktop images - Click <strong>Push Updates</strong>, select the assignment(s) from the list and click <strong>OK</strong> to push the updates.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Before you push updates to your existing assignments, it is recommended that you first create a test assignment and push updates to it in order to confirm that all features are working as expected.</td>
</tr>
<tr>
<td></td>
<td>- RDS images</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> If you updated the image using the Update Agent Software function, click <strong>Push Updates</strong>, select the farm from the list and click <strong>OK</strong> to push the updates.</td>
</tr>
<tr>
<td></td>
<td>- If you updated the image but did not use the Update Agent Software function, no action is needed. The updates are pushed automatically when you re-publish an updated image.</td>
</tr>
<tr>
<td>Download Bootstrap</td>
<td>Downloads an encrypted bootstrap file for you to deploy to your image(s).</td>
</tr>
<tr>
<td></td>
<td>You will be prompted to enter a password of 8-20 ASCII characters containing at least one each of the following: lowercase letter, uppercase letter, number, and symbol (@#$%^&amp;*). Do not use non-ASCII characters in the password.</td>
</tr>
<tr>
<td>Refresh Password</td>
<td>Creates a new default password to be used for bootstrapping images.</td>
</tr>
<tr>
<td></td>
<td>If you do this after having downloaded a bootstrap file but before applying the bootstrap file using keytool, then the resultant agents will not be able to pair. Therefore, it is recommended that you download the bootstrap file again after refreshing the password.</td>
</tr>
</tbody>
</table>

**Update an Instant Clone Image**

You can update an Instant Clone image and the assignments based on the image.

Unlike a Traditional Clone image that can be updated after being published (take offline, make changes, and republish), an Instant Clone image must be duplicated and the new image updated and added to the relevant assignments.

**Procedure**

1. Select **Inventory > Images** from the menu to open the Images page.
2. Select the check box for the image, click the "..." button, and select **Duplicate** from the drop-down menu.
   
   The system creates a duplicate of the image.

   **Note** This process can take some time, so plan accordingly.

3. Make the necessary changes to the duplicate image and publish it.
4. When the new image has been published, edit each of the assignments based on the original image so that they use the duplicate image instead. See **Edit an Assignment**.

   As users log out of their sessions, the VMs in each assignment will be synced with the new image.
5. [Optional] Delete the original image by selecting it on the Images page, clicking the "..." button, and selecting **Delete** from the drop-down menu.
Automatically Sync Images Across Desktop Managers

If you have multiple Desktop Managers registered to a Tenant within the same Data Center, the Image Sync option can automatically sync images across the desktop managers.

Image Sync is disabled by default, and can be enabled/disabled for each Tenant by your VMware representative.

When enabled, Image Sync automatically does the following.

- Duplicates new images across Desktop Managers, so you do not have to manually clone and import the images.
- Syncs changes to images across Desktop Managers, so you do not have to make the changes on all copies.

Note the following:

- Images that you created before Image Sync is enabled will not be automatically synced. You will have to take them offline and then republish them for the sync to occur.
- If you have synced images and then have the feature disabled, for each of the synced images an additional image will appear in the list with a name similar to the synced image.

Create an Image

Create a new desktop image from the Images page.

Note This process takes approximately 30 minutes. Be sure you allow sufficient time to complete it before you begin.

Procedure

1. Select Inventory > Images.
   The Images page displays.
2. Click New.
   The New Image dialog displays.
3. In the Desktop field, start typing the first few letters of the template name.
   All desktops that can be converted to an image will display. Note that it takes approximately five minutes after the template import for the inventory to display.
4. Select the desktop name when it appears.

Note Make sure that the desktop is powered on prior to conversion.
5 Confirm that the Agent Status has changed to Active, indicating that agent pairing has occurred. This should happen within approximately 30 seconds.

**Note** You must have the most recent agents installed for agent pairing to succeed. If you are using older versions of the agents, ensure that the DaaS Agent is manually configured and bootstrapped for agent pairing to complete.

6 For Instant Clone, select **Yes** to create an Instant Clone image or **No** to create a Traditional Clone image. For information about types of images, see Chapter 8 Images.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Instant Clone</td>
<td>Image type that uses VMware’s NGVC technology to create VMs instantly for an assignment.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Windows Server operating systems are not supported for Instant Clone assignments, so you should not create Instant Clone images from Windows Server template VMs. Although the image can be created with the Instant Clone Agent installed and desktops can be provisioned from it, the desktops will not launch successfully for users.</td>
</tr>
<tr>
<td>Traditional Clone</td>
<td>Proprietary image type that does full image cloning when creating assignments.</td>
</tr>
</tbody>
</table>

7 Enter the required information as described below.

The image type you selected above affects the fields that display.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Image Name</td>
<td>Name for the new image</td>
</tr>
<tr>
<td>Domain</td>
<td>[Instant Clone only] Select domain from the drop-down list</td>
</tr>
<tr>
<td>Company Name</td>
<td>Your company name</td>
</tr>
<tr>
<td>TimeZone</td>
<td>Your time zone</td>
</tr>
<tr>
<td>Username</td>
<td>Admin user for required desktop domain</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> This field displays for Instant Clone images only if your VMware representative has enabled the Image Sync feature.</td>
</tr>
<tr>
<td>Password/Verify Password</td>
<td>Password for the Admin user.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> This field displays for Instant Clone images only if your VMware representative has enabled the Image Sync feature.</td>
</tr>
</tbody>
</table>

8 Click **Publish**.

The publishing process takes approximately 40 minutes to complete. If successful, the Image task shows as Complete.

**Note** Do not restore a VM to a snapshot taken prior to the bootstrapping process. If the agent has been already boot-strapped, this will prevent the agent from communicating as it should.
If the publish operation fails:

- Select **Monitor > Activity** and locate the failed job.
- Correct the problem that caused the failure.
- Select **Inventory > Images** and select the check box next to the image.
- Click ... and select **Convert to Desktop**.
- Repeat the steps above to re-publish the image.

## Update Agent Software for an Image

Use the agent update feature to update agent software for an image and push updates to assignments.

The agent update feature allows automated update of all the agents in an image in a single operation.

- The system makes regular contact with the VMware CDS software distribution network and downloads agent updates automatically to a file share that you have set up on a local machine. The update files are then automatically imported into the system and made available for images.
- The availability of updates is indicated on the Images page, where you can apply them to images.
- Your VMware representative can adjust the interval between scans for new agents and the wait time for scans after tenant startup if you request it.

### Prerequisites

- You must have created an Agents file share and added it to Horizon Cloud. This means that you select Agents for the file share type when you create the file share. Agents file shares are used only for importing agent update files. See **Managing File Shares**.
- The image must already have DaaS Agent 16.6.0.4408091 or higher in order to perform a DaaS Agent update.
- The image must already have Horizon Agent 7.0.3.4612900 or higher in order to perform a Horizon Agent update.

### Procedure

1. Click **Inventory > Images**.
   
   The Images page displays, with a blue dot appearing next to the name of any assignment that has agent updates available.
   
   - If you hover over a blue dot, a popup displays indicating the agent updates available for that image.
   
   - The system selects the latest versions of each agent by default, but you can open each drop-down to view all available versions.

2. Select the check box an image. You can only update agents for one image at a time.

3. Click **Update Agent**.
   
   The Agent Update dialog displays.
4 On the Software tab, select the agent(s) to update and click **Next**.

5 On the Agreements tab, select the **Agree** radio button for each agreement you wish to accept and click **Next**. The system skips the update for any item for which you do not accept the agreement.

6 (Optional) On the Command Line tab, add any command line options. For details regarding command line options, see the documentation for the relevant agent.

   **Note** There are currently no command line options available for the DaaS Agent.

7 Click **Finish**.

   - A message displays at the top of the page indicating that the update has started.
   - The system creates a clone of the image and updates the agent(s) on the clone image.

   **Note** the following:

   - Desktops are updated in batches, which cannot be larger than 30. If the assignment has 30 or fewer desktops, all desktops in the assignment will be updated together. Your VMware representative can adjust the batch size if you request it.
   - If a desktop has an active session, the user will be warned five minutes before the update occurs.
   - If a user attempts to login into a desktop that is being updated, the login will be unsuccessful and the user will receive a message that the desktop is not available.

   You can view the progress of the update task by selecting **Monitor > Activity**. The task description indicates the agent being updated and the assignment on which the update is being performed. If the task is not successful within 24 hours, it fails.

8 Push updates based on the clone image. For more information, see Managing Images.

9 (Optional) Delete the original image and rename the clone image with the original image name.

**Build Your Own Template**

Before you create an image, you must first prepare the desktop template.

The process of building the template includes the following:

- Install and configure agents
- Set up direct connection to desktop VMs (optional)
- Optimize the display (optional)

**Installing and Configuring Agents**

It is important that you install and configure agents on the template VM in the correct order.

Before you begin installing the agents, perform the tasks described in Prepare the Template VM for Agent Installation.
Prepare the Template VM for Agent Installation

Before installing the agent software required for connecting to connect to desktops, complete the following pre-installation steps.

**Procedure**

1. Uninstall all software components related to all other protocols.
   
   **Important:** You must uninstall all software components related to all other protocols (e.g. HDX, RGS). If you do not uninstall these other protocol components, your template will be corrupted and you will no longer successfully boot into Windows. This warning does not apply to RDP; the presence of RDP components does not cause problems.

2. Update VMware Tools.

3. Make sure that port 443 is not being used by any other software, or use a non-standard port.

4. Make sure that the following ports are open to TCP and/or UDP traffic as indicated:

<table>
<thead>
<tr>
<th>Port(s)</th>
<th>Source</th>
<th>Destination</th>
<th>TCP</th>
<th>UDP</th>
</tr>
</thead>
<tbody>
<tr>
<td>4172 (PCoIP)</td>
<td>Access Point</td>
<td>VM</td>
<td>P</td>
<td>P</td>
</tr>
<tr>
<td>443 (View</td>
<td>Tenant Appliance</td>
<td>VM</td>
<td>P</td>
<td></td>
</tr>
<tr>
<td>communication)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>32111 (PCoIP)</td>
<td>Access Point</td>
<td>VM</td>
<td>P</td>
<td></td>
</tr>
<tr>
<td>22443 (HTML Access)</td>
<td>Access Point</td>
<td>VM</td>
<td>P</td>
<td></td>
</tr>
<tr>
<td>443 (HTML Access)</td>
<td>Access Point</td>
<td>T/VM</td>
<td>P</td>
<td></td>
</tr>
<tr>
<td>8443 (HTML Access)</td>
<td>Access Point</td>
<td>VM</td>
<td>P</td>
<td></td>
</tr>
<tr>
<td>4172 (PCoIP)</td>
<td>Access Point</td>
<td>VM</td>
<td>P</td>
<td>P</td>
</tr>
<tr>
<td>80 (redirects to 443)</td>
<td>Access Point</td>
<td>T/VM</td>
<td>P</td>
<td></td>
</tr>
</tbody>
</table>

What to do next

Install the Horizon Agent. See [Installing the Horizon Agent](#)

**Installing the Horizon Agent**

After you have completed the preparation steps, you can install the Horizon Agent on the template VM.

There are three possible scenarios when installing the Horizon Agent:

- Install on desktop (Windows 7, Windows 8, Windows 8.1, Windows 10)
- Install on server (Windows Server 2008 R2, Windows Server 2012 R2) as Personal Desktop (Non-RDSH)
- Install on server (Windows Server 2008 R2, Windows Server 2012 R2) as RDSH Role

**Note** If you have not installed the most recent version of the Horizon Agent, this can cause problems with creating RDS pools. In this case, when you create a new RDS pool, the system can allow you to select HTML Access (Blast) as a protocol, but this selection will not be applied to the pool even though it appears to have been applied successfully.

## Install the Horizon Agent on a Windows Desktop

You can install the Horizon Agent on a Windows 7, Windows 8, Windows 8.1, or Windows 10 desktop.

**Procedure**

1. Download the latest Horizon Agent from the Myvmware download site. Note that there are separate downloads for 32-bit and 64-bit operating systems.
2. Double-click the Horizon Agent installation file (file name is: VMware-viewagent-x86_64-x.y.z-nnnnnnnn.exe for the 64-bit installer).
3. Perform a custom installation with the following options:
   - Deselect VMware Horizon View Composer Agent.
   - Select VMware Horizon Instant Clone Agent.
   - Select vRealize Operations Desktop Agent.
4. Restart the virtual machine when prompted.

**What to do next**

- For improved security regarding the use of the Horizon Agent, disable weak ciphers in SSL and TLS, which requires you to edit the Group Policy Object (GPO) of the Active Directory server. See the appropriate Horizon Agent documentation for information about disabling weak ciphers in SSL/TLS, such as in the VMware Horizon 7 documentation set.

- **Install the DaaS Agent**

## Install the Horizon Agent on Windows Server as Personal Desktop (Non-RDSH)

You can install the Horizon Agent on Windows Server 2008 R2 or 2012 R2 as a personal desktop.

**Procedure**

1. Download the latest Horizon Agent from VMware’s website (https://my.vmware.com). Note that there are separate downloads for 32-bit and 64-bit operating systems.
2. Double-click the Horizon Agent installation file (file name is: VMware-viewagent-x86_64-x.y.z-nnnnnnnn.exe for the 64-bit installer).
3. Select the option to install the Horizon Agent in desktop mode.
Perform a custom installation with the following options:

- Deselect VMware Horizon View Composer Agent.
- Select vRealize Operations Desktop Agent.

Restart the virtual machine when prompted.

What to do next

- For improved security regarding the use of the Horizon Agent, disable weak ciphers in SSL and TLS, which requires you to edit the Group Policy Object (GPO) of the Active Directory server. See the appropriate Horizon Agent documentation for information about disabling weak ciphers in SSL/TLS, such as in the VMware Horizon 7 documentation set.

- Install the DaaS Agent

Install the Horizon Agent on Windows Server as an RDSH Role

You can install the Horizon Agent on Windows Server 2008 R2, 2012 R2, or 2016 as an RDSH role.

**Note** To install the Horizon Agent in this scenario, you MUST run the command line install and cannot use the default “double click” GUI.

**Procedure**

1. Add the Remote Desktop Services role.
   
   a. Select **Start > Administrative Tools > Server Manager** to open the Server Manager.
   
   b. Select **Roles** and then select **Add Roles** in the right pane.
   
   c. Click **Next**.
   
   d. Select the check box for Remote Desktop Services and click **Next**.
   
   e. Click **Next**.
   
   f. Select the check box for Remote Desktop Session Host and click **Next**.
   
   g. Click **Next**.
   
   h. Select the appropriate Authentication Level, and then click **Next**.

   The Specify Licensing Mode page appears.
i Specify the licensing mode, and then click Next.  
The Select User Groups Allowed Access To This RD Session Host Server page appears.

j Add your Users or User Groups, and then click Next.  
The Configure Client Experience page appears.

k Make desired settings, and then click Next.  
The Confirm Installation Selections page appears.

l Confirm your selections. If something is incorrect, click Previous to return to the previous steps and change the settings. Click Install.  
The Installation Progress page appears. The installation takes a few minutes to finish. The Installation Results page appears, and asks for restart.

m Click Close.  
A dialog appears, asking for confirmation for restart.

n Click Yes to restart the server.

o When the server comes back, log in again.  
The Resuming Configuration page appears. It takes a few seconds to resume configuration. The Installation Results page appears.

p Click Close to complete the installation.  
The Server Manager window appears.

q Click Roles and confirm that the Remote Desktop Services role is installed.

2 Download the latest Horizon Agent from VMware’s website (https://my.vmware.com). Note that there are separate downloads for 32-bit and 64-bit operating systems.

3 Run the following on the command line as an administrator user:  
   VMware-viewagent-x86_64-x.y.z-nnnnnnn.exe /v "VDM_SKIP_BROKER_REGISTRATION=1"

4 Perform a custom installation with the following options:
   ◆ Select vRealize Operations Desktop Agent.

5 Restart the virtual machine when prompted.

What to do next

- For improved security regarding the use of the Horizon Agent, disable weak ciphers in SSL and TLS, which requires you to edit the Group Policy Object (GPO) of the Active Directory server. See the appropriate Horizon Agent documentation for information about disabling weak ciphers in SSL/TLS, such as in the VMware Horizon 7 documentation set.

- Install the DaaS Agent
Install the DaaS Agent
After installing the Horizon Agent, install the DaaS Agent.

**Note**  The manual configuration required for older versions of the DaaS Agent is no longer necessary.

**Procedure**

1. Download the most recent DaaS Agent installer file from the Myvmware.com download site.
2. Run the installer on the template virtual machine.

**What to do next**

Install the App Volumes Agent

Install the App Volumes Agent
After you have installed the Horizon Agent, you can install the App Volumes Agent.

**Procedure**

1. Download the most recent App Volumes Unified Agent Installer file from the Myvmware.com download site.
2. Run the installer on the template virtual machine.
3. During installation, deselect localhost and specify the primary tenant IP address and port 3443 (for example: 192.168.12.12:3443).
4. Edit the registry to configure add the IP address of the secondary tenant appliance for High-Availability:
   a. Run regedit and navigate to HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\svservice\Parameters.
   b. Add a String Value called 'Manager2' with a value of <TA2 IP Address>:3443 (for example: 192.168.12.12:3443).

Configuring VMware Horizon Smart Policies

A Horizon Cloud environment supports using VMware Horizon smart policies to control the end users' virtual desktops. These smart policies provide policy-driven control over the behavior of features such as USB redirection, virtual printing, clipboard redirection, client drive redirection, and PCoIP display protocol features on the virtual desktops. By using these smart policies, you can have policies that take effect only if certain conditions are met. For example, you can configure a policy that disables the client drive redirection feature if a user connects to a remote desktop from outside your corporate network.

For a detailed description of VMware Horizon smart policies and instructions on how to use them, see Using Smart Policies in the VMware Horizon documentation or the VMware Horizon smart policies information in the VMware Horizon document titled Configuring Remote Desktop Features in Horizon 7.
These smart policies require use of User Environment Manager software and the App Volumes Unified Agent Installer software to install the required agents. You can download the software from the VMware Downloads page. Obtain version User Environment Manager 9.1 or later. For User Environment Manager system requirements and complete installation instructions, see the User Environment Manager product documentation. For detailed information and best practices for using User Environment Manager and App Volumes with your environment, see the document titled VMware App Volumes with Horizon Cloud Application Delivery Best Practices and Operations Procedures at vmware.com.

After you have completed installation and configuration of User Environment Manager and its Management Console as described in the previously mentioned documents, to configure a smart policy on your master virtual machine (VM), you need to perform the following steps on that master VM.

- If you have not done so already, run the App Volumes Unified Agent Installer, as described in Install the App Volumes Agent. The User Environment Manager agent is installed on the VM in that process. The User Environment Manager FlexEngine client is installed with that agent component.
- Define the VMware Horizon smart policy using the User Environment Manager Management Console.
  For descriptions of the VMware Horizon smart policy settings you can select in User Environment Manager, see Horizon Smart Policy Settings in the VMware Horizon 7 documentation.
  - Add conditions that must be met for the policy to take effect, as described in Adding Conditions to Horizon Smart Policy Definitions in the VMware Horizon documentation.

For examples of using Horizon smart policies, see Reviewer's Guide for View in VMware Horizon 7: Smart Policies document at vmware.com.

Adding Conditions to Horizon Smart Policy Definitions describes the use of Horizon Client property conditions in the smart policies. Predefined Horizon Client properties correspond to ViewClient_registry keys. Not all of the predefined properties used in Horizon 7 are applicable in a Horizon Cloud environment. The properties that are not applicable are:

- ViewClient_Broker_Pool_Tags
- ViewClient_Broker_Tags
- ViewClient_Launch_Matched_Tags
- ViewClient_Broker_DNS_Name

In a Horizon Cloud environment configured using Unified Access Gateway, the broker sets the following gateway-related properties by default to these values as follows:

- If your Unified Access Gateway is external, then the ViewClient_Broker_GatewayLocation property is set to External and ViewClient_Broker_GatewayType property is set to AP.
- If your Unified Access Gateway is internal, then the ViewClient_Broker_GatewayLocation property is set based on the Internal Networks list and the ViewClient_Broker_GatewayType property is set to AP.

**Note** The Internal Networks list is created by your service provider and is displayed on the General Settings page.

Using a Unified Access Gateway with your Horizon Cloud environment is a best practice. However, if you do not have a Unified Access Gateway, the broker sets the ViewClient_Broker_GatewayLocation property based on the Internal Networks list and sets the ViewClient_Broker_GatewayType property to None.

### Configure Administrator Direct Access to Desktops

Administrators can now connect to desktops using their domain accounts, instead of being required to have local admin access.

To allow this, a new DaaS Direct Connect Users group will be created during the DaaS Agent installation. This group does not have local administration rights, but is allowed to connect to the desktop through the Helpdesk Console or using a direct RDP connection.

There are two methods for adding a user to the DaaS Direct Connect Users group:

- Update the image.
- using a GPO policy on the tenant appliance.

**Note** This procedure is separate from the template VM configuration process and can be performed at any time.

To add members by updating the image:

1. Join the image VM to the domain and then restart it.
2. Add domain user(s) to the DaaS Direct Connect Users group.
3. Publish the image and provision desktops. All desktops created using the image will now have the group member details.

To add members using a GPO policy on the tenant appliance:

1. Create a new GPO.
2. Right-click on the GPO and select `Edit`.
4. Right-click `Restricted Groups` and select `Add Group`.
5. In the Add Group dialog, enter DaaS Direct Connect Users and click `OK`.
6. In the properties dialog, enter members in the 'Members of this group' text box, click `Add`, and then click `OK`.
7 Close the Group Policy Management Editor and the Group Policy Management Console.
8 Link the newly created GPO to the domain.

**Optimizing the Display**

Perform the tasks linked below to optimize the display on the template VM.

**Add the PCoIP Group Policy Settings**

You can add the PCoIP Group Policy Settings to the local computer policy environment.

To configure the group policies, you must first add the .adm template file to the Local Computer Policy configuration on this VM.

**Procedure**

1 On the template VM, click **Start > Run**.
2 Type `gpedit.msc` and click **OK**.
   
The Local Group Policy Editor console opens.
3 Confirm that you can connect to the View Connection Server from this VM.
4 In the navigation pane, select **Local Computer Policy > Computer Configuration**.
5 Right-click **Administrative Templates**.

   **Note**  Do not select Administrative Templates under **User Configuration**.
6 Select **Add/Remove Templates**.
7 In the **Add/Remove Templates** dialog, click **Add**.
8 Download the `pcoip_policies.adm` file from the Horizon DaaS Library on salesforce.com.
9 Click **Open**.
10 Close the Add/Remove Templates window.

The PCoIP group policy settings are added to the Local Computer Policy environment on the desktop system and are available for configuration.

**Add the HTML Access (Blast) Group Policy Settings**

You can add the HTML Access (Blast) Group Policy Settings to the local computer policy environment.

**Procedure**

1 Download the View GPO Bundle .zip file from the VMware Horizon download site.

   The file is named VMware-Horizon-View-Extras-Bundle-x.x.x-yyyyyyy.zip, where x.x.x is the version and yyyyyyy is the build number. All ADM and ADMX files that provide group policy settings for View are available in this file.
2 Copy the file to your Active Directory server and unzip the file.

   The HTML Access GPOs are included in the Blast-enUS.adm ADM Template file.

3 On the Active Directory server, edit the GPO.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows 2008 or 2012</td>
<td></td>
</tr>
<tr>
<td></td>
<td>a Select Start &gt; Administrative Tools &gt; Group Policy Management.</td>
</tr>
<tr>
<td></td>
<td>b Expand your domain, right-click the GPO that you created for the group policy settings, and select Edit.</td>
</tr>
<tr>
<td>Windows 2003</td>
<td></td>
</tr>
<tr>
<td></td>
<td>a Select Start &gt; All Programs &gt; Administrative Tools &gt; Active Directory Users and Computers.</td>
</tr>
<tr>
<td></td>
<td>b Right-click the OU that contains your View desktops and select Properties.</td>
</tr>
<tr>
<td></td>
<td>c On the Group Policy tab, click Open to open the Group Policy Management plug-in.</td>
</tr>
<tr>
<td></td>
<td>d In the right pane, right-click the GPO that you created for the group policy settings and select Edit.</td>
</tr>
</tbody>
</table>

   The Group Policy Object Editor window appears.

4 In the Group Policy Object Editor, right-click Administrative Templates under Computer Configuration and then select Add/Remove Templates.

5 Click Add, browse to the Blast-enUS.adm file, and click Open.

6 Click Close to apply the policy settings in the ADM Template file to the GPO.

   The VMware Blast folder appears in the left pane under Administrative Templates > Classic Administrative Templates.

7 Configure the HTML Access group policy settings.

8 Make sure your policy settings are applied to the remote desktops.
   a Run the gupdate.exe command on the desktops.
   b Restart the desktops.

Configure Policy Settings for Display

You can configure policy settings to optimize the display on the template VM.

Make the following settings in the Overrideablepolicy group.

Procedure

1 Enable “Turn off Build-to-Lossless feature” by selecting the check box.

2 Enable “Configure PCoIP image quality levels”
   - Set Minimum Image Quality to 30.
   - Set Maximum Image Quality to 70.
   - Set Maximum Frame Rate to 16.
Enabling 3D Graphics

You can enable 3D graphics on a per-assignment basis.

Support for 3D graphics is provided using Soft 3D, also known as vSGA (see pages 3-4 of the VMware white paper on Graphics Acceleration for more information). In order for you to use 3D graphics feature, the following must be true:

- Virtual hardware version must be 8 or higher.
- Desktop must have the Windows Aero theme.
- Servers must have appropriate hardware installed.

**Note** Consult the latest PCoIP recommendations when configuring desktops with this feature.
Farms in Horizon Cloud

A farm is a collection of Microsoft Remote Desktop Services (RDS) hosts that provide multiple users with session-based desktops and applications. Farms simplify the management of the RDS hosts. You can create farms to serve groups of users that vary in size or have different desktop or application requirements.

Before you can assign session-based desktops or remote applications to end users, you must create the farms to serve those desktops and applications. A farm can provide either session-based desktops or remote applications.

Use the Farms page in the Administration Console to manage your farms. You navigate to the Farms page using the Inventory icon.

This chapter includes the following topics:

- Create a Farm
- Managing Farms in Horizon Cloud
Create a Farm

You create farms using the Farms page.

**Note**  The RDS-enabled assignable image is also referred to as an RDS host or an RDSH (Remote Desktop Services Host) image.

**Prerequisites**

Verify that you have at least one assignable image listed on the Images page, that image has an RDS-enabled Windows server operating system, and that image is located in the node in which you want to create the farm. You cannot create a farm in a node without an assignable image available in that node.

Decide whether this farm will serve session-based desktops or remote applications.

**Procedure**

1. In the Administration Console, navigate to **Inventory > Farms**.

2. Click **New**.

   The New Farm wizard opens.

3. In the wizard’s Definition step, complete the fields and make your selections as appropriate and then click **Next**.

   **Note**  You might have to use the scroll bar to see all of the required fields.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a name for this farm.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter an optional description.</td>
</tr>
</tbody>
</table>
### Option Description

**Farm Type**
Specify the type of asset this farm will provide to end users:
- Select **Desktops** to use this farm to provide session-based desktops.
- Select **Applications** to use this farm to provide access to remote applications. After an applications farm is created, you can use the New Application workflow's **Auto-scan from Farm** option to import applications from the farm's servers into your application inventory.

**Pod**
This option only displays if your data center is configured with multiple pods. Pods contain specific assignable images and server model capacities for assignments. You can only create assignments from images in the same pod.

**Image**
Select the assignable RDSH image.

**Preferred Protocol**
Select a default display protocol you want the end user sessions to use. Circumstances might occur that cause another protocol to be used instead of the default protocol. For example, the client device does not support the default protocol or the end user overrides the default protocol selection.

**Preferred Client Type**
Select the preferred client type used when end users launch their session-based desktops from the Workspace™ ONE™ platform's portal, either a Horizon Client or a browser for HTML Access.

**Domain**
Select the Active Directory domain registered with your environment.

**Join Domain**
Select **Yes** so that the farm's server instances are automatically joined the domain when they are created.

**Servers**
Specify the number of servers you want in this farm.

**Sessions per Server**
Specify the number of concurrent end user sessions per server that this farm will allow.

**Important** In this release, you cannot update this number after the farm is created. As a result, you must choose judiciously the value you select here.

### Optionally configure the advanced properties.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>VM Names</strong></td>
<td>Name for all of the server VMs created for this farm, which will have a number appended to it, for example, win2016-1, win2016-2, etc. The name must start with a letter and can contain only letters, dashes, and numbers.</td>
</tr>
<tr>
<td><strong>Computer OU</strong></td>
<td>Active Directory Organizational Unit where the server VMs are to be located. For example, O=RootOrgName, DC=DomainComponent, DC=eng, and so on. The entries must be comma-separated with no spaces in between. If you need to use nested Organization Units, see Working with Nested Organizational Units</td>
</tr>
<tr>
<td><strong>Run Once Script</strong></td>
<td>(Optional) Location of scripts that you want run after system preparation completes.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Session Timeout Interval| This is the amount of time the end users’ sessions can be idle before the system forces a log off from the session-based desktops or applications that are served by this farm. This timeout applies to the logged-in session to the underlying Windows operating system. This timeout interval is separate from the timeout settings that govern the end users’ Horizon Client or HTML Access logged-in session.  

**Caution** When the system forces the log off in the underlying Windows operating system session, any unsaved data is lost. To prevent an unintended loss of data, set this interval high enough to accommodate the business needs of your end users.  

**Note** If no user activity occurs before the timeout interval is reached, a message indicates that the user will be logged off if they do not click **OK** in the next 30 seconds. If the logoff occurs, any unsaved user data, such as documents or files, is lost. |
| Enable Windows Hot-Plug | (Optional) Keep the default **No** setting to prevent end users from dynamically adding or removing external devices from their virtual desktops, such as CD/DVD drives, Ethernet adapters, and similar device types.  

**Caution** Setting this toggle to **Yes** can result in users accidentally interfering with connectivity to the virtual desktops if the users dynamically remove the networks cards (NICs) or other operational components by mistake. Even though you might choose to enable this setting for special cases, such as supporting the use of thumb drives in your virtual desktops, be aware that the setting is enabled for all such plug-and-play devices in the resulting desktops. |
In the wizard's Management step, complete the fields and make your selections as appropriate and then click Next.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rolling Maintenance</td>
<td>Select the maintenance type, either according to a time cadence (Scheduled) or based on user sessions to this farm's servers (Session). When Scheduled is selected, configure the maintenance cadence, either daily or weekly. If you choose a daily recurrence, specify the hour at which the maintenance will start. If you choose a weekly recurrence, specify both the day of the week and the hour. When Session is selected, specify the number of sessions at which the farm should begin rolling maintenance. Note: Sessions which are logged off within 15 minutes are not counted for the purposes of the rolling maintenance calculations, to prevent restarting or rebuilding the servers based on a count of short running sessions. In the Concurrent Quiescing Servers field, specify the number of servers that can be in the quiescing state at the same time. When a server is in quiescing state, the server continues to work for the user sessions already connected to that server, but it does not accept any new user connections.</td>
</tr>
</tbody>
</table>
| Server Action      | Select the action that the system should perform on the servers undergoing maintenance.  
- With Restart, the server VMs are restarted.  
- With Rebuild, the server VMs are first deleted and then reprovisioned from their RDS desktop image. |
| Timeout Handling   | Configure how you want the system to handle certain types of user sessions. Note: The user sessions governed by these settings are the user logins to the Windows operating system session of the RDS session desktop or application. These sessions are not the user logins in Horizon Client, Horizon HTML Access, or Workspace ONE. The user's session begins when the user authenticates to the Windows operating system that underlies the session-based desktop or the remote application that is served from this farm's servers.  
- Empty Session Timeout - For applications farms, select how the system should handle idle user sessions, whether to never timeout idle sessions or to timeout after a specified number of minutes. Idle timeouts are based on the activity on the endpoint device, not on the session-based desktop or application. If you specify to timeout an idle session, select what happens when the timeout period is up: whether to disconnect the session or log the user off. When a session is disconnected, the session is disconnected from the network and preserved in memory. When a session is logged off, the session is not preserved in memory, and any unsaved documents are lost.  
- Log Off Disconnected Sessions - Select when the system logs the user off of a disconnected session.  
- Max Session Lifetime - Specify the maximum number of minutes the system should allow for a single user session. |

In the wizard's Summary step, review the settings and then click Submit to begin creating the farm.
The system starts creating the farm. You can monitor the progress using the Activity page. When the farm's status shows a green dot on the Farms page:

- If you created a desktops farm, you can use it to create a session-based desktop assignment.
- If you created an applications farm, you can use it to load applications from the servers' underlying RDS-enabled operating system into your Horizon Cloud applications catalog.

<table>
<thead>
<tr>
<th>Status</th>
<th>Farm Name</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>✔</td>
<td>Demo2</td>
<td>Remote Desktops</td>
</tr>
<tr>
<td>✔</td>
<td>Demo1</td>
<td>Remote Desktops</td>
</tr>
</tbody>
</table>

**What to do next**

If you created a desktops farm, you would next create a session-based desktop assignment for your end users by following the steps in Create an RDSH Session Desktop Assignment.

If you created an applications farm, you would next scan that farm to load applications into Horizon Cloud and then create an applications assignment so your end users can use the remote applications from that farm.

For more information, see Chapter 7 Applications, Importing New Applications from an RDSH Farm Using Auto-Scan from Farm, and Manually Adding Custom Applications from an RDSH Farm.

**Managing Farms in Horizon Cloud**

You can perform several actions on the farms listed on the Administration Console's Farms page.

**Actions You Can Perform on the Farms Page**

At a page level, you can select the check box next to an existing farm and click one of the buttons to perform its associated action on the farm.

**Edit**

Clicking this button launches a wizard in which you can change certain settings, such as the farm's power management settings, the minimum and maximum number of servers the farm can have, and so on. The wizard is similar to the New Farm wizard, with read-only fields for those settings that cannot be changed for an existing farm. For detailed descriptions of the fields, see Create a Farm.

Alternatively, instead of using the Edit button, you can click the farm's name and update the settings from the farm's summary page.

**Take Offline**

Clicking this button opens a window in which you can select to take a farm offline for maintenance.
**Bring Online**
Clicking this button opens a window in which you can select to bring an offline farm back online.

**Delete**
You use this button to delete the selected farm. However, before you can delete a farm using this button, you must delete any assignments that are using the farm. You can view the assignments that are using the farm by navigating to the Assignments page and sorting on its Farms column.

---

**Note**
Deleting the farm deletes all of the farm's underlying server VMs. When a farm is deleted, all of that farm's logged activity is removed from the Activity page.

---

**Actions You Can Perform Within a Farm's Detailed Pages**
From the Farms page, you can click a farm's name to see its detailed pages. Initially the Summary page is displayed.

### Summary page
The Summary page displays the farm's current settings. For each page section, you can click **Edit** to change those settings that the system allows to be updated for an existing farm. Some settings cannot be changed on a farm after it is created, such as its node.

### Servers page
The Servers page displays the existing server instances in the farm. The actions you can perform on a selected server are power on or off (depending on the server's current state) and delete.

---

**Horizon Cloud with Hosted Infrastructure Administration**
VMware, Inc. 92
The Sessions page displays the farm's existing user sessions. When you select a session, you can disconnect it or log the user off the session. When you click Disconnect, you force the user's session to be disconnected. No message is sent to the user that the session is disconnecting. When you click Log Off, a message is displayed to the user with a grace period in which the user can save documents before the session ends.

The System Activity page displays activity in the farm due to system actions, such as expanding the farm.

The User Activity page displays activity in the farm due to user actions, such as logging on and logging off sessions provided by the farm.

**Manage Servers in a Farm**

You can perform certain actions on the individual servers in a farm.

**Procedure**

1. Click Inventory > Farms.
   
The Farms page displays.

2. Click the name of a farm on the list.
   
The farm details page displays.

3. Click Servers at the top of the page.
   
The Servers tab displays, showing a list of servers for the farm. You can filter, refresh, and export the list using the controls to the top right of the page.

   You can perform the following actions by selecting one or more servers and clicking one of the buttons at the top of the page.

   **Note** Server status must be green to perform these actions.
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power Off</td>
<td>Shuts down the selected servers.</td>
</tr>
<tr>
<td></td>
<td>• You can select more than one server at a time.</td>
</tr>
<tr>
<td></td>
<td>• You can only shut down VMs that do not have active user sessions.</td>
</tr>
<tr>
<td>Power On</td>
<td>Starts up the selected powered-off servers.</td>
</tr>
<tr>
<td>Delete</td>
<td>Deletes the selected server.</td>
</tr>
<tr>
<td>Launch Console</td>
<td>Launches a console so that you can log in to the virtual machine.</td>
</tr>
</tbody>
</table>
The Capacity page displays current desktop capacity and usage information.

At the top of the page you can:

- Filter information displayed by Data Center and Pod using the drop-down menus.
- Download a report in .csv format by clicking the Download Full Service Report link.

The main area of the page has two sections, described below.

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Desktop Model</td>
<td>Shows the total standard capacity, with number of units used for each desktop model and units available.</td>
</tr>
<tr>
<td>Storage Types</td>
<td>Shows total storage, with amount used for different storage types and amount free. Click on the arrow icon below Storage GB to see the storage broken down by individual volumes.</td>
</tr>
</tbody>
</table>
Imported VMs

Imported VMs are unmanaged VMs with supported operating systems imported into Horizon Cloud to be converted into images or migrated to dedicated desktop assignments.

You can perform the following actions using buttons at the top of the page.

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rename</td>
<td>Select a VM and click Rename. Enter a new name in the field and click Save. Note: For this action to be successful, the selected VM must be paired with the tenant using Agent Pairing and the DaaS Agent must be in Active state.</td>
</tr>
</tbody>
</table>
| Shutdown | Shuts down the VM(s).  
  ▪ You can select more than one VM at a time.  
  ▪ VM status must be green.  
  ▪ You can only shut down VMs that do not have active user sessions. |
| Restart  | Performs a 'graceful' restart of the VM(s), allowing you to recover hung VMs without loss of data. If this does not work, it may be necessary to use the Reset menu option, which performs a hard reset of the VM and can result in data loss.  
  ▪ You can select more than one VM at a time.  
  ▪ VM status must be green. |

You can perform the following actions by clicking the "..." button and making a selection from the drop-down menu.

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Suspend</td>
<td>Suspends the selected VM.</td>
</tr>
<tr>
<td>Resume</td>
<td>Resumes operation of the selected VM.</td>
</tr>
<tr>
<td>Power On</td>
<td>Powers on the selected VM.</td>
</tr>
<tr>
<td>Power Off</td>
<td>Powers off the selected VM.</td>
</tr>
<tr>
<td>Reset</td>
<td>Resets the selected VM.</td>
</tr>
<tr>
<td>Log Off</td>
<td>Logs off the selected VM.</td>
</tr>
<tr>
<td>Disconnect</td>
<td>Disconnects the selected VM.</td>
</tr>
<tr>
<td>Convert to Image</td>
<td>Converts the selected VM to an image.</td>
</tr>
<tr>
<td>Delete</td>
<td>Permanently deletes the selected VM.</td>
</tr>
<tr>
<td>Migrate to Utility VMs</td>
<td>Moves the VM to the Utility VMs page. See Managing Utility VMs.</td>
</tr>
<tr>
<td>Action</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Launch Console</td>
<td>Launches a console for the selected desktop. This option is disabled if the VM is powered off or if more than one VM is selected.</td>
</tr>
<tr>
<td>Migrate to Assignment</td>
<td>Associates the VM(s) with a dedicated desktop assignment. In the Migrate VM(s) dialog, select an assignment in the Assignment Name field and click Migrate.</td>
</tr>
<tr>
<td></td>
<td>- VMs can only be migrated to dedicated desktop assignments with the same Desktop Manager ID.</td>
</tr>
<tr>
<td></td>
<td>- Selected VM must be paired with the tenant using Agent Pairing and DaaS Agent must be in Active state.</td>
</tr>
<tr>
<td></td>
<td>- Registry entry &quot;Use SVI=0&quot; is required. This is already present with DaaS Agent 17.1.x and View Agent 7.1, but will have to be added manually for older agents.</td>
</tr>
</tbody>
</table>
## Settings

Edit a variety of settings for your system.

Select the Settings icon to access these options.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>General Settings</td>
<td>Displays settings for networks, domain, etc. You can edit settings from this page, and upload certificates. See Edit General Settings.</td>
</tr>
<tr>
<td>Active Directory</td>
<td>View and edit Active Directory details. See Edit an Active Directory Domain.</td>
</tr>
<tr>
<td>Roles &amp; Permissions</td>
<td>Edit Roles and Permissions. See Edit Roles and Permissions.</td>
</tr>
<tr>
<td>Infrastructure</td>
<td>Create file shares and perform actions on existing file shares. See Managing File Shares.</td>
</tr>
<tr>
<td>Storage Management</td>
<td>View list of AppStacks in your environment. See Managing Storage.</td>
</tr>
<tr>
<td>Getting Started</td>
<td>Opens the Getting Started wizard. See Chapter 3 Getting Started Wizard.</td>
</tr>
<tr>
<td>Utility VMs</td>
<td>Opens the Utility VMs page. See Managing Utility VMs.</td>
</tr>
<tr>
<td>2 Factor Auth</td>
<td>Configure 2 Factor authentication for end users. See 2 Factor Authentication.</td>
</tr>
</tbody>
</table>

This chapter includes the following topics:

- Edit General Settings
- Active Directory
- Edit Roles and Permissions
- Managing File Shares
- Managing Storage
- Managing Utility VMs
- 2 Factor Authentication
- Identity Management
Edit General Settings

You can edit general settings and upload certificates from the General Settings page.

Procedure

1. Select Settings > General Settings.
2. Click Edit.
3. Make changes for these settings.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Networks</td>
<td>The Networks list shows a list of your currently used network(s). This list is not editable. Contact your service provider to edit or add network(s).</td>
</tr>
<tr>
<td>Default Domain</td>
<td>Default domain that you are editing.</td>
</tr>
</tbody>
</table>
| Session Timeout         | - Client Heartbeat Interval - Controls the interval between Horizon Client heartbeats and connected state. These heartbeats report to the broker the amount of idle time that has passed. Idle time occurs when no interaction occurs with the end point device, as opposed to idle time in the desktop session. In large desktop deployments, setting the activity heartbeats at longer intervals might reduce network traffic and increase performance.  
  - Client Idle User - Maximum time that a user can be idle while connected to the tenant. When this maximum is reached, the user is disconnected from all active Horizon Client Desktop sessions. The user must re-authenticate to re-access the Horizon Client.  
  
  **Note** Set the Client Idle User timeout to be at least double the Client Heartbeat Interval to avoid unexpected disconnects from desktops.  
  - Client Broker Session - Maximum time that a Horizon Client instance can be connected to the tenant before its authentication expires. The timeout count starts each time you authenticate. When this timeout occurs, you can continue to work. If you perform an action that causes communication to the broker, such as changing settings, the system requires you to re-authenticate and log back in to the desktop.  
  
  **Note** The Client Broker Session timeout must be at least equal to the sum of the Client Heartbeat Interval and the Client Idle User timeout.  
  - User Portal Timeout - How long you can be on the User Portal when you try to broker a connection before you need to log in again.                                                                                                                                 |
| User Portal Configuration| This feature is deprecated.                                                                                                                                                                          |
| Monitoring              | Enable User Session Information - This feature allows user and domain data to be used by the Cloud Monitoring Service (CMS) for reports on the Reports page. If it is disabled, the following are not provided:  
  - The Unique User Summary feature of the Utilization report  
  - The Session History report  
  
  **Note** The agents on the virtual machines (RDSH and VDI) need outbound Internet access so they can send the data to Horizon Cloud.                                                                                                                                 |
| HTML Access             | Cleanup credentials when tab is closed - Controls whether to delete credentials of the broker session when a HTML Access portal connection tab is closed. |
### Option Description

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Agent Pairing</strong></td>
<td>Sets a policy on the tenant which determines the access of legacy (pre-16.6.0) and 16.6.0 agents. Options are as follows:</td>
</tr>
<tr>
<td></td>
<td>- 15.3 Compatibility Mode - Allows legacy and 16.6.0 agents to be paired with Desktop Manager. This is the default setting for upgraded setups.</td>
</tr>
<tr>
<td></td>
<td>- 16.6 Upgrade Mode - Restricts legacy agents, but allows un-bootstrapped 16.6.0 agents on persistent desktops and bootstrapped 16.6.0 agents. This</td>
</tr>
<tr>
<td></td>
<td>mode does not restrict desktops that are already paired using 15.3.x agents unless the desktop or agent service is restarted.</td>
</tr>
<tr>
<td></td>
<td>- 16.6 Mode - Allows only bootstrapped 16.6.0 agents to be paired. This mode does not restrict desktops that are already paired using 15.3.x agents</td>
</tr>
<tr>
<td></td>
<td>or un-bootstrapped 16.6.0 agents unless the desktop or DaaS agent service is restarted. This is the default setting for fresh installs.</td>
</tr>
<tr>
<td></td>
<td>When to change this setting:</td>
</tr>
<tr>
<td></td>
<td>- Change from 15.3 Compatibility Mode to 16.6 Upgrade Mode only when there are no longer any pre-16.6 agents in the system BUT there are some</td>
</tr>
<tr>
<td></td>
<td>dedicated desktops from before the upgrade with their agents upgraded to 16.6.</td>
</tr>
<tr>
<td></td>
<td>- Change from 15.3 Compatibility Mode to 16.6 Mode when there are no longer any pre-16.6 agents or 16.6 agents that are paired with legacy credentials.</td>
</tr>
<tr>
<td></td>
<td>Once the 16.6 mode is enabled, only VMs creating using bootstrapped images will work.</td>
</tr>
<tr>
<td><strong>RDSH Farm</strong></td>
<td>Defines policy parameters for RDSH farms.</td>
</tr>
<tr>
<td></td>
<td>- Session Lifetime Reminder Message - This message reminds users that they will be logged off after a specified grace period.</td>
</tr>
<tr>
<td></td>
<td>Default message is “Dear user, your session has reached the maximum lifetime, you will be logged off in {0} minutes”. The value specified in</td>
</tr>
<tr>
<td></td>
<td>the Grace Period field replaces {0} in the message seen by the user.</td>
</tr>
<tr>
<td></td>
<td>- Grace Period - Interval of time after which user is logged off following Session Lifetime Reminder Message.</td>
</tr>
<tr>
<td><strong>Contact Info</strong></td>
<td>Contact information for administrator and technical support.</td>
</tr>
</tbody>
</table>

4. Click **Save**.

### Active Directory

This section describes the procedures for registering and configuring Active Directory domains.

Note the following:

- You must register your first Active Directory domain before you can work with any other services. All services are locked until you complete these tasks.
- When you are defining groups of users or administrators, always select ‘Security’ for the Active Directory group type, as Distribution groups are not supported.
Register Your First Active Directory Domain

You must complete the configuration by registering Active Directory, completing the domain join, and adding the Super Administrator.

**Note** You must complete the entire Active Directory registration process before you can work with any other services. All services are locked until you complete these tasks.

**Note** When you have completed the domain registration, do not move any groups from one organizational unit (OU) to another. Doing so will cause login failures for users.

If you click **Cancel** before you complete the registration, you can click **Edit** at any time from the Getting Started page to continue with registration.

**Prerequisites**
- The Active Directory infrastructure must be synchronized to an accurate time source.
- If you have external or forest trusts, root domains must be registered. For more information, see [External and Forest Trusts](#).
- The LDAP bind account is treated by the system as a Super Admin user, so this account should not be shared with any user that does not have Super Admin privileges. For example, if there is another product that also needs an LDAP bind account, a new LDAP account should be created for this purpose so whoever has the new account cannot log in as Super Admin.

**Procedure**

1. On the Getting Started page, select **General Setup** and then click **Configure** next to Active Directory.

2. In the Register Active Directory dialog box, provide the requested registration information.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NETBIOS Name</td>
<td>Active Directory domain name</td>
</tr>
<tr>
<td>DNS Domain Name</td>
<td>Fully qualified Active Directory domain name</td>
</tr>
<tr>
<td>Protocol</td>
<td>Not editable; LDAP is the only choice</td>
</tr>
<tr>
<td>Bind Username</td>
<td>Domain administrator</td>
</tr>
<tr>
<td>Bind Password</td>
<td>Domain administrator password</td>
</tr>
</tbody>
</table>

3. Enter information for Auxiliary Account #1.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bind Username</td>
<td>Domain administrator</td>
</tr>
<tr>
<td>Bind Password</td>
<td>Domain administrator password</td>
</tr>
</tbody>
</table>

**Note** Username and password must exist in the Active Directory or the account will not be added successfully.
4 Click **Advanced Properties**.

5 Enter information the Advanced Properties fields.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port</td>
<td>The default for this field is 389. You should not need to modify this field unless you are using a non-standard port.</td>
</tr>
<tr>
<td>Domain Controller IP</td>
<td>(Optional) Specify a single preferred domain controller IP address if you want AD traffic to use a specific domain controller.</td>
</tr>
<tr>
<td>Context</td>
<td>This option is auto-populated based on the DNS Domain Name information provided earlier.</td>
</tr>
</tbody>
</table>

6 Click **Domain Bind**.

**Note** If you see an error stating that the auxiliary account information you entered is invalid, then after completing the Domain Join process below you will need to add a valid auxiliary account by editing the Domain Bind information. See **Edit an Active Directory Domain**.

7 Provide the domain join information.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Join Username</td>
<td>Domain administrator</td>
</tr>
<tr>
<td>Join Password</td>
<td>Domain administrator password</td>
</tr>
<tr>
<td>Primary DNS Server IP</td>
<td>IP address of primary DNS Server</td>
</tr>
<tr>
<td>Secondary DNS Server IP</td>
<td>(Optional) IP of secondary DNS Server</td>
</tr>
<tr>
<td>Default OU</td>
<td>Default organizational unit</td>
</tr>
</tbody>
</table>

8 Click **Save**.

9 In the Add Super Administrator dialog box, use the Active Directory search function to select the AD administrator group to administer the application.

10 Click **Save**.

11 If the domain bind or domain join process fail, you must restart the registration process.

   a Restart the browser.
   
   b Log in first using your My VMware account.
   
   c Log in to the Active Directory account using the domain service (bind) account login and password.
   
   d Continue with the domain join process.

**What to do next**

If desired, you can set up True SSO (single sign-on). See **Configure True SSO for an Active Directory Domain**.
Register Additional Active Directory Domains

You can optionally register additional Active Directory domains to assign management roles or provide assignments to users in those domains.

**Note**  When you have completed the domain registration, do not move any groups from one organizational unit (OU) to another. Doing so will cause login failures for users.

If you click **Cancel** before you complete the registration, you can click **Edit** at any time from the Getting Started page to continue with registration.

**Prerequisites**

- The Active Directory infrastructure must be synchronized to an accurate time source.
- If you have external or forest trusts, root domains must be registered. For more information, see [External and Forest Trusts](#).
- The LDAP bind account is treated by the system as a Super Admin user, so this account should not be shared with any user that does not have Super Admin privileges. For example, if there is another product that also needs an LDAP bind account, a new LDAP account should be created for this purpose so whoever has the new account cannot log in as Super Admin.

**Procedure**

1. In the Administration Console, select **Settings > Active Directory**.
2. Click **Register**.
3. In the Register Active Directory dialog box, provide the requested registration information.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NETBIOS Name</td>
<td>Active Directory domain name</td>
</tr>
<tr>
<td>DNS Domain Name</td>
<td>Fully qualified Active Directory domain name</td>
</tr>
<tr>
<td>Protocol</td>
<td>Not editable; LDAP is the only choice</td>
</tr>
<tr>
<td>Bind Username</td>
<td>Domain administrator</td>
</tr>
<tr>
<td>Bind Password</td>
<td>Domain administrator password</td>
</tr>
</tbody>
</table>

4. Enter information for Auxiliary Account #1.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bind Username</td>
<td>Domain administrator</td>
</tr>
<tr>
<td>Bind Password</td>
<td>Domain administrator password</td>
</tr>
</tbody>
</table>

**Note**  Username and password must exist in the Active Directory or the account will not be added successfully.

5. Click **Advanced Properties**.
6  Enter information the Advanced Properties fields.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port</td>
<td>The default for this field is 389. You should not need to modify this field unless you are using a non-standard port.</td>
</tr>
<tr>
<td>Domain Controller IP</td>
<td>(Optional) Specify a single preferred domain controller IP address if you want AD traffic to use a specific domain controller.</td>
</tr>
<tr>
<td>Context</td>
<td>This option is auto-populated based on the DNS Domain Name information provided earlier.</td>
</tr>
</tbody>
</table>

7  Click **Domain Bind**.

**Note** If you see an error stating that the auxiliary account information you entered is invalid, then after completing the Domain Join process below you will need to add a valid auxiliary account by editing the Domain Bind information. See **Edit an Active Directory Domain**.

8  Provide the domain join information.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Join Username</td>
<td>Domain administrator</td>
</tr>
<tr>
<td>Join Password</td>
<td>Domain administrator password</td>
</tr>
<tr>
<td>Primary DNS Server IP</td>
<td>IP address of primary DNS Server</td>
</tr>
<tr>
<td>Secondary DNS Server IP</td>
<td>(Optional) IP of secondary DNS Server</td>
</tr>
<tr>
<td>Default OU</td>
<td>Default organizational unit</td>
</tr>
</tbody>
</table>

9  Click **Save**.

10 In the Add Super Administrator dialog box, use the Active Directory search function to select the AD administrator group to administer the application.

11 Click **Save**.

12 If the domain bind or domain join process fail, you must restart the registration process.
   a  Restart the browser.
   b  Log in first using your My VMware account.
   c  Log in to the Active Directory account using the domain service (bind) account login and password.
   d  Continue with the domain join process.

**What to do next**

If desired, you can set up True SSO (single sign-on). See **Configure True SSO for an Active Directory Domain**.

**Edit an Active Directory Domain**

You can edit an Active Directory domain after initial setup.
Procedure

1. Select Settings > Active Directory.

The Active Directory page displays.

2. If you have multiple Active Directories configured, select the one you want to edit from the list on the left.

3. Click **Edit** next to Domain Bind to edit domain bind information.

The Edit Active Directory dialog displays.

4. Edit information as desired in the fields described below.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NETBIOS Name</td>
<td>[Not editable] Active Directory domain name</td>
</tr>
<tr>
<td>DNS Domain Name</td>
<td>Fully qualified Active Directory domain name</td>
</tr>
<tr>
<td>Protocol</td>
<td>[Not editable] LDAP is the only choice</td>
</tr>
<tr>
<td>Bind Username</td>
<td>Domain administrator. Edit only if new username is set up in Active Directory first.</td>
</tr>
<tr>
<td>Bind Password</td>
<td>Domain administrator password. Edit only if new password is set up in Active Directory first.</td>
</tr>
</tbody>
</table>

5. Click **Advanced Properties**.

6. Edit information as desired in the following Advanced Properties fields.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port</td>
<td>The default for this field is 389. You should not need to modify this field unless you are using a non-standard port.</td>
</tr>
<tr>
<td>Domain Controller IP</td>
<td>(Optional) Specify a single preferred domain controller IP address if you want AD traffic to use a specific domain controller.</td>
</tr>
<tr>
<td>Context</td>
<td>This option is auto-populated based on the DNS Domain Name information provided earlier.</td>
</tr>
</tbody>
</table>

7. Make changes to auxiliary bind accounts as described below.

- Add an auxiliary bind account:
  1. Click the **Add Auxiliary Bind Account** link.
  2. Enter username and password for the account.

  **Note** Username and password must exist in the Active Directory or the account will not be added successfully.

- Change password for an auxiliary bind account:
  1. Confirm that the password for the account has already been changed in the Active Directory.
  2. Click the Change Account Password link for the account (for example, Change Account #1 Password).
3 Enter the new password.

**Note** You cannot change the bind username for an auxiliary bind account. Instead, you need to remove the account and add it with the new username.

- Remove an auxiliary bind account by clicking the **Remove** link next to the account.

  **Note** You cannot remove an auxiliary bind account if it is the last active service account remaining.

8 Click **Domain Bind** to save changes.

9 Click **Edit** next to Domain Join to edit domain join information.

The Domain Join dialog displays.

10 Edit domain join information as desired.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Join Username</td>
<td>Domain administrator. Edit only if new username is set up in Active Directory first.</td>
</tr>
<tr>
<td>Join Password</td>
<td>Domain administrator password. Edit only if new password is set up in Active Directory first.</td>
</tr>
<tr>
<td>Primary DNS Server IP</td>
<td>IP address of primary DNS Server</td>
</tr>
<tr>
<td>Secondary DNS Server IP</td>
<td>(Optional) IP of secondary DNS Server</td>
</tr>
<tr>
<td>Default OU</td>
<td>Default organizational unit</td>
</tr>
</tbody>
</table>

11 Click **Save**.

12 In the Add Super Administrator dialog box, make any desired change and click **Save**.

Use the Active Directory search function to select the AD administrator group to administer the system.

**What to do next**

If desired, you can set up True SSO (single sign-on). See **Configure True SSO for an Active Directory Domain**.

**Configure True SSO for an Active Directory Domain**

After you have registered an Active Directory domain, you can configure True SSO on it.

**Prerequisites**

Before configuring True SSO, you must first have at least one Identity Manager configured. See **Identity Management**.

**Procedure**

1 In the Administration console, select **Settings > Active Directory**.
2 Click the **Download Pairing Token** link under True SSO Configuration.
   The pairing_bundle.7z file downloads to your Downloads folder.

3 Unzip the two certificate template files from the bundle.
   Note the location of the files. You will need these when configuring the Enrollment Server in the last phase in the infrastructure setup.

4 Set up the required infrastructure as described in **Infrastructure Setup for True SSO**.

5 On the Active Directory page in the Administration console, click **Add** next to True SSO Configuration.
   The True SSO Config dialog displays.
   **Note** Because you already downloaded the pairing token on the Active Directory page, you can ignore the **Download Pairing Token** link in this dialog.

6 Enter the name of your enrollment server in the Primary Enrollment Server field and click the **Test Pairing** button next to the field.
   The other required fields are auto-populated.

7 Click **Save**

8 To configure a Secondary Enrollment Server for high-availability, do the following.
   a Repeat the process described in **Set up the Enrollment Server** on a second machine.
   b Edit the True SSO configuration and add the second ES address in the Secondary Enrollment Server field, and then test the pairing.
   c Save the configuration again.

The configuration information now appears on the Active Directory page under True SSO Configuration.

**Infrastructure Setup for True SSO**

This section includes the procedures for setting up the infrastructure required for True SSO configuration.

Before adding a True SSO configuration on the Active Directory page, complete the tasks below.

- Install and configure a Windows Server Certificate Authority (CA)

  **Note** The procedures in this section are for Windows Server 2012 R2. Very similar steps can be followed on Windows Server 2008 R2.

- Set Up a certificate template on the CA

- Set up the Enrollment Server (ES)

The CA will issue certificates on behalf of the users, and those certificates will be used to log the users in to their allocated desktops. Horizon Cloud appliance will ask the ES to issue certificates on behalf of users. The ES will generate the requested certificate on behalf of the requested user via the CA and return it to the Horizon Cloud appliance.
Install and Configure a Windows Server 2012 R2 Certificate Authority

You can set up a Windows Server 2012 Certificate Authority (CA) using the Service Manager wizard.

The following are standard steps to set up a Microsoft CA. They are detailed here in a simple form suitable for use in a lab environment, but for a real production system it is recommended that you follow industry best practice for CA configuration.

If you need further guidance about setting up a CA, please check out the standard Microsoft technical references: Active Directory Certificate Services Step-by-Step Guide and Install a Root Certification Authority.

**Note**  The procedures in this topic are for Windows Server 2012 R2. Very similar steps can be followed on Windows Server 2008 R2.

**Procedure**

1. On the Server Manager Dashboard, click **Add Roles and Features** to open the wizard, and then and click **Next**.

2. On the Select Installation Type page, select Role-based or feature-based installation and click **Next**.

3. On the Server Selection page, leave defaults and click **Next**.

4. On the Server Roles page:
   b. In the dialog, select Include management tool (if applicable) and click **Add Features**.
   c. Click **Next**.

5. On the Features page, click **Next**.

6. On the AD CS page, click **Next**.

7. On the Role Services page, select Certification Authority and click **Next**.

8. On the Confirmation page, select Restart the destination server automatically is required and click **Install**.

   Installation Progress displays. When the installation is complete, a URL link displays, allowing you to configure the newly installed CA as “Configure Active Directory Certificate Services” on the destination server.

9. Click on the configuration link to launch the configuration wizard.

10. On the Credentials page, enter user credentials from Enterprise Admin group and click **Next**.

11. On the Role Services page, select CA and click **Next**.

12. On the Setup Type page, select Enterprise CA and click **Next**.

13. On the CA Type page, select Root or Subordinate CA as appropriate (in this example it is a Root CA) and click **Next**.

14. On the Private Key page, select Create a new private key and click **Next**.
15 On the Cryptography page, enter information as follows.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cryptographic Provider</td>
<td>RSA#Microsoft Software Key Storage Provider</td>
</tr>
<tr>
<td>Key Length</td>
<td>4096 (or another length if you prefer)</td>
</tr>
<tr>
<td>Hash Algorithm</td>
<td>SHA256 (or another SHA algorithm if you prefer)</td>
</tr>
</tbody>
</table>

16 On the CA Name page, configure as preferred or accept defaults and click **Next**.

17 On the Validity Period page, configure as preferred and click **Next**.

18 On the Certificate Database page, click **Next**.

19 On the Confirmation page, review the information and click **Configure**.

20 Complete the configuration process by performing the following tasks (run all commands from the command prompt).

   a Configure CA for non-persistent certificate processing

        certutil -setreg DBFlags +DBFLAGS_ENABLEVOLATILEREQUESTS

   b Configure CA to ignore offline CRL errors

        certutil -setreg ca\CRLFlags +CRLF_REVCHECK_IGNORE_OFFLINE

   c Restart the CA service

        net stop certs
        net start certsvc

**What to do next**

Set Up a Certificate Template on the CA

**Set Up a Certificate Template on the CA**

You can configure the certificate template on the CA. The certificate template is the basis for the certificates that the CA generates.

**Prerequisites**

Install and Configure a Windows Server 2012 R2 Certificate Authority
Procedure

1  Create a new Universal Security Group.

   This allows you to have a single Security Group to which you can assign the permissions required for issuing certificates on behalf of users. All the computers where VMware Enrollment Servers are installed can inherit those permissions by becoming a member of this group.

   a  Click Start and type dsa.msc.

      The Active Directory Users and Computers dialog displays.

   b  In the tree, right-click the Users folder for the domain controller and select New > Group.

      The New Object - Group dialog displays.

   c  In the Group Name field, enter a name for the new group. For example, TrueSSO Enrollment Servers.

   d  Make settings as described below.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group scope</td>
<td>Universal</td>
</tr>
<tr>
<td>Group type</td>
<td>Security</td>
</tr>
</tbody>
</table>

   e  Click OK.

      The new group appears in the tree in the Active Directory Users and Computers dialog.

   f  Right-click the group and select Properties.

   g  On the Member Of tab, add the computer where the Enrollment Server will be installed, and then click OK.

   h  Restart the computer(s) where the Enrollment Server(s) will be installed

2  Configure certificate template.

   a  Select Control Panel > Administrative Tools > Certificate Authority.

   b  In the tree, expand the local CA name.

   c  Right-click on the Certificate Templates folder and select Manage.

      The Certificate Templates Console displays.

   d  Right-click on the Smartcard Logon template and select Duplicate Template.

      The Properties of New Template dialog displays.
e Enter information on the tabs of the dialog as described below.

<table>
<thead>
<tr>
<th>Tab</th>
<th>Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compatibility</td>
<td>• Select 'Show resulting changes' check box</td>
</tr>
<tr>
<td></td>
<td>• Certification Authority - Windows Server 2008 R2</td>
</tr>
<tr>
<td></td>
<td>• Certificate recipient - Windows 7 / Server 2008 R2</td>
</tr>
<tr>
<td>General</td>
<td>• Template display name - Name of your choice. For example, True SSO Template.</td>
</tr>
<tr>
<td></td>
<td>• Template name - Name of your choice. For example, True SSO Template.</td>
</tr>
<tr>
<td></td>
<td>• Validity period - 1 hours</td>
</tr>
<tr>
<td></td>
<td>• Renewal period - 0 weeks</td>
</tr>
<tr>
<td>Request Handling</td>
<td>• Purpose - Signature and smartcard logon</td>
</tr>
<tr>
<td></td>
<td>• Select 'For automatic renewal of smart card certificates . . .' check box</td>
</tr>
<tr>
<td></td>
<td>• Select 'Prompt the user during enrollment' radio button</td>
</tr>
<tr>
<td>Cryptography</td>
<td>• Provider Category - Key Storage Provider</td>
</tr>
<tr>
<td></td>
<td>• Algorithm name - RSA</td>
</tr>
<tr>
<td></td>
<td>• Minimum key size - 2048</td>
</tr>
<tr>
<td></td>
<td>• Select 'Requests can use any provider available . . .' radio button</td>
</tr>
<tr>
<td></td>
<td>• Request hash - SHA256</td>
</tr>
<tr>
<td>Subject Name</td>
<td>• Select 'Build from this Active Directory Information' radio button</td>
</tr>
<tr>
<td></td>
<td>• Subject name format - Fully distinguished name</td>
</tr>
<tr>
<td></td>
<td>• Select 'User principal name (UPN) check box</td>
</tr>
<tr>
<td>Server</td>
<td>• Select 'Do not store certificates and requests in the CA database' check box</td>
</tr>
<tr>
<td>Issuance Requirements</td>
<td>• Require the following for enrollment - Select 'This number of authorized signatures' and enter 1</td>
</tr>
<tr>
<td></td>
<td>• Policy type required in signature - Application policy</td>
</tr>
<tr>
<td></td>
<td>• Application policy - Certificate Request Agent</td>
</tr>
<tr>
<td></td>
<td>• Require the following for enrollment - Valid existing certificate</td>
</tr>
<tr>
<td>Security</td>
<td>In the upper part of the tab select the new group you created. Then in the lower part of the tab select 'Allow' for Read and Enroll permissions.</td>
</tr>
</tbody>
</table>

f Click OK.

3 Issue template for True SSO.

a Right-click again on the Certificate Templates folder and select **New > Certificate Template to Issue**.

The Enable Certificate Templates dialog displays.

b Select TrueSsoTemplate and click OK.
4 Issue Enrollment Agent template.
   a Right-click again on the Certificate Templates folder and select New > Certificate Template to Issue.
      The Enable Certificate Templates dialog displays.
   b Select the Enrollment Agent computer and click OK.
      
      Note: This template must have the same security settings as the template issued in the previous step.

The CA is now set up and configured with a certificate template suitable for use with True SSO.

What to do next
Set up the Enrollment Server

Set up the Enrollment Server
The Enrollment Server (ES) is a Horizon Cloud component that you install on a Windows Server machine as the last step in setting up infrastructure for True SSO. By deploying the Enrollment Agent (Computer) certificate onto the server, you are authorizing this ES to act as an Enrollment Agent and generate Certificates on behalf of users.

Prerequisites
Set Up a Certificate Template on the CA

Procedure
1 Install the Enrollment Server.
   a Download the Enrollment Server .exe file from the My VMware site. The file name should be similar to VMware-HorizonCloud-TruessoEnrollmentServer-x86_64-7.3.0-xxxxx.exe.
   b Confirm that the system is running Windows Server 2008 R2 or 2012 R2 machine and has a minimum of 4GB memory.
   c Run the installer and follow the wizard.
2 Deploy the Enrollment Agent (Computer) Certificate.
   a Open the Microsoft Management Console (MMC).
   b On the File menu, click Add/Remove Snap-in.
   c Under Available snap-ins, double-click Certificates.
   d Select Computer account and click Next.
   e Select Local computer and click Finish.
   f On the Add or Remove Snap-ins dialog, click OK.
g In the MMC, right-click the Personal folder under Certificates and select **All Tasks > Request New Certificates**.

h In the Certificate Enrollment dialog, select the check box for the Enrollment Agent (Computer) and click **Enroll**.

3 Import the pairing bundle.

a In the MMC, right-click the Certificates sub-folder under the VMware Horizon Cloud Enrollments Server Trusted Roots folder and select **All Tasks > Import**.

b Click **Next**.

c Navigate to the location where you unzipped the certificate files from the pairing_bundle.7z bundle.

d Import the two certificate files one at a time.

e Click **Next**, then click **Finish**.

**What to do next**

Complete the remaining steps to configure True SSO in the administration console. See [Configure True SSO for an Active Directory Domain](#).

**External and Forest Trusts**

The system supports traversing external (or forest) trusts between domains in different forests.

This includes:

- Assignment/entitlement of users/groups in one forest to resources in a different forest.
- Support for one-way trusts.

For this functionality to work, you must do the following.

- Register all domains from all forests that contain accounts and desktops you wish to use.
- Register forest root domains from both sides of a forest trust. This is required to allow the tenant to connect to the forest roots and decode the relevant TDO. This requirement holds even if there are no DaaS desktops or users in the forest root domains.
- Enable global catalog for at least one of the registered domains in each forest. For optimal performance all registered domains should have global catalog enabled.
- To entitle groups from different forests to a desktop, register at least one universal group from each forest. Entitlement/assignment using domain local groups is not supported. As a result, the system filters out FSPs from 'member' attribute DN and tokenGroups.
- Follow a hierarchical structure with regard to DNS name and root naming context for forest domains. For example, if the parent domain is called example.edu, a child domain could be called vpc.example.edu but not vpc.com.
Avoid having a domain from an externally trusted forest with a clashing NETBIOS name, as such domains will be excluded. The registered NETBIOS name will always take precedence over a clashing NETBIOS name found during enumeration of a trusted forest's domains.

**Edit Roles and Permissions**

You can edit roles that were previously configured.

**Procedure**

1. Select **Settings > Roles & Permissions**.
   
   The Roles & Permissions page displays.
   
   There are two default roles, shown below.

<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Super-Administrator</td>
<td>Users with this role have access to all functionality and can save changes.</td>
</tr>
<tr>
<td>Demo-Administrator</td>
<td>Users with this role have access to all functionality but cannot save any changes.</td>
</tr>
</tbody>
</table>

2. Select a role from the Roles list and click **Edit**.

3. In the edit dialog, use the Active Directory search function to select a group for the role and click **Save**.

   **Note**  Do not add the same group to both the Super-Administrator role and the Demo-Administrator role. Doing so can cause users in that group not to have full access to all expected functions.

**Managing File Shares**

You can set up file shares to import data into the user interface.

- You create a file share on a separately-managed machine outside of the user interface and then add it on the Infrastructure page.

- After the file share has been added to the system, the contents are imported either automatically or manually, depending on the functionality involved.

- There are two types of file shares that support various functions:

<table>
<thead>
<tr>
<th>Type</th>
<th>Used For:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agents</td>
<td>Agent software update - Agent files are automatically downloaded into the file share, imported in the system, and made available on the Assignments page. See <a href="#">Update Agents for an Assignment</a>.</td>
</tr>
<tr>
<td>Applications/Images</td>
<td>App Volumes integration - You copy AppStacks into the file share and then import them on the Infrastructure page. See <a href="#">Import Applications Using App Volumes</a>.</td>
</tr>
</tbody>
</table>
Create a File Share

You can create a file share outside of the user interface.

Procedure

1. Create a Windows folder following the usual procedure.
   - If this is an Agent file share (that is, a file share for use with Agent Software Update), you must name the folder 'agentFiles'. Later the system will create several subfolders, only two of which you use. These subfolders are described below.

<table>
<thead>
<tr>
<th>Subfolder Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cdsClient</td>
<td>This folder will contain agent files downloaded automatically from the upgrade server that your VMware representative has configured for you.</td>
</tr>
<tr>
<td>hotpatch</td>
<td>This folder will contain any agent files that you manually put into it. You will not have any need to do this unless specifically asked to do so by your VMware representative.</td>
</tr>
</tbody>
</table>

   - If this is an Applications/Images file share, the name can be anything you choose.

2. Make the following settings for the file share folder:
   - Confirm that the file share is joined to the tenant domain.
   - Enable sharing.
   - Add a domain user to the permissions.

3. Note the following information, which you will need when adding the file server in the user interface:
   - Username and password of the domain user used you added in the previous step.
   - Source path of the file share folder.

What to do next

Add the file share in the user interface. See Add a File Share on the Infrastructure Page.

Add a File Share on the Infrastructure Page

After you create a file share outside of the user interface, you can add it on the Infrastructure page.

Note  When you add a file share, the contents of the file share (agent files or AppStacks) are imported into the system. If you put new content into the file share later, you can import that content using the Import function.

Prerequisites

In order to add a file share on the Infrastructure page, you must first create it outside of the user interface. See Create a File Share.
Procedure

1. Select **Settings > Infrastructure** and click **File Share**.
2. Click **New**.
3. Provide the required information in the New File Share dialog box.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the file share.</td>
</tr>
<tr>
<td>Domain</td>
<td>Domain of the file share. Select from the drop-down list.</td>
</tr>
<tr>
<td>Username</td>
<td>Admin user for the file share.</td>
</tr>
<tr>
<td>Password</td>
<td>Admin password for the file share.</td>
</tr>
<tr>
<td>Type</td>
<td>Type of file share. Select Agents or Applications/Images, depending on what the file share contains.</td>
</tr>
<tr>
<td></td>
<td>- Agents file shares are used only to import agent software updates.</td>
</tr>
<tr>
<td></td>
<td>- Applications/Images file shares are used to import AppStacks.</td>
</tr>
<tr>
<td>Source Path</td>
<td>Network path to file share.</td>
</tr>
<tr>
<td>Destination Pod</td>
<td>[Applications/Images Type only] This field only displays if you have multiple pods on the tenant. Select the pod from the drop-down list.</td>
</tr>
</tbody>
</table>

4. Click **Save**.

**Edit a File Share**

You can edit the name, source path, and destination pod of a file share.

Procedure

1. Select **Settings > Infrastructure**.
2. Select the check box next to the file share to edit.
3. Click **Edit** and make your changes.
4. Click **Save**.

**Remove a File Share**

You can remove a file share on the Infrastructure page.

Procedure

1. On the Infrastructure page, select the file share to remove.
2. Click **Remove** and confirm you want to remove the file share.
   
   The file share no longer appears in the list.

**Import the Contents of a File Share**

You can import the contents of a file share on the Infrastructure page.
**Procedure**

1. Select **Settings > Infrastructure**.
2. On the Infrastructure page, select the file share.
3. Click the ". . . " button and select **Import**.
   - In most cases, all files will be imported automatically, and will be available on the appropriate page of the user interface.

<table>
<thead>
<tr>
<th>File Type</th>
<th>User Interface Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agents</td>
<td>Assignments page (see Update Agents for an Assignment).</td>
</tr>
<tr>
<td>AppStacks</td>
<td>Applications page.</td>
</tr>
</tbody>
</table>

- If there is an agent file being delivered as a hotpatch, you will be prompted to enter the hash value that you received from your VMware representative. You have no need to use this functionality unless specifically asked to by your VMware representative.

**Managing Storage**

On the Storage Management page, you can manage AppStacks.

Select **Settings > Storage Management** to open the Storage Management page.

**Manage AppStacks**

The AppStacks tab of the Storage Management page lists all AppStacks on the tenant.

- To free up storage space, you can delete an AppStack by selecting it in the list and clicking the **Delete** button.

  **Note**  You cannot delete an AppStack that has active user sessions.

- You can filter the list or refresh the page using the controls in the top right of the page.

**Managing Utility VMs**

Utility VMs are discovered VMs with unsupported operating systems used for infrastructure services such as DHCP.

You can perform the following actions using buttons at the top of the page.
<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rename</td>
<td>Select a VM and click Rename. Enter a new name in the field and click Save.</td>
</tr>
<tr>
<td>Note</td>
<td>For this action to be successful, the selected VM must be paired with the tenant using Agent Pairing, and the DaaS Agent must be in Active state.</td>
</tr>
<tr>
<td>Shutdown</td>
<td>Shuts down the VM(s).</td>
</tr>
<tr>
<td></td>
<td>▪ You can select more than one VM at a time.</td>
</tr>
<tr>
<td></td>
<td>▪ VM status must be green.</td>
</tr>
<tr>
<td></td>
<td>▪ You can only shut down VMs that do not have active user sessions.</td>
</tr>
<tr>
<td>Restart</td>
<td>Performs a ‘graceful’ restart of the VM(s), allowing you to recover hung VMs without loss of data. If this does not work, it may be necessary to use the Reset menu option, which performs a hard reset of the VM and can result in data loss.</td>
</tr>
<tr>
<td></td>
<td>▪ You can select more than one VM at a time.</td>
</tr>
<tr>
<td></td>
<td>▪ VM status must be green.</td>
</tr>
</tbody>
</table>

You can perform the following actions by clicking the "..." button and making a selection from the drop-down menu.

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Suspend</td>
<td>Suspends the selected VM.</td>
</tr>
<tr>
<td>Resume</td>
<td>Resumes operation of the selected VM.</td>
</tr>
<tr>
<td>Power On</td>
<td>Powers on the selected VM.</td>
</tr>
<tr>
<td>Power Off</td>
<td>Powers off the selected VM.</td>
</tr>
<tr>
<td>Reset</td>
<td>Resets the selected VM.</td>
</tr>
<tr>
<td>Log Off</td>
<td>Logs off the selected VM.</td>
</tr>
<tr>
<td>Disconnect</td>
<td>Disconnects the selected VM.</td>
</tr>
<tr>
<td>Migrate To Imported VMs</td>
<td>Moves the VM to the Imported VMs page. See Chapter 11 Imported VMs.</td>
</tr>
</tbody>
</table>

2 Factor Authentication

The system supports RSA SecurID and Radius authentication for internal users.

To enable 2 Factor Authentication for users on your internal network, see Set Up Authentication with RADIUS and Set Up Authentication with RSA SecurID.

Set Up Authentication with RADIUS

You can use RADIUS to enable 2 Factor Authentication for end users.

Note Make sure that primary and secondary tenant appliance IP addresses are registered as clients in the RADIUS server. Obtain the tenant appliance IP addresses from your VMware representative.

Procedure

1. Select Settings > 2 Factor Auth.
2 Configure the authentication.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2nd factor Auth Method</td>
<td>Select Radius.</td>
</tr>
<tr>
<td>Maintain Username</td>
<td>Select Yes to maintain the username during authentication. The user who is</td>
</tr>
<tr>
<td></td>
<td>attempting to authenticate must have the same username credentials for RSA</td>
</tr>
<tr>
<td></td>
<td>and Domain Challenge. If you select No, the username field is not locked and</td>
</tr>
<tr>
<td></td>
<td>the user can enter a different name.</td>
</tr>
<tr>
<td>External Connections Only</td>
<td>Select NO to configure 2 Factor Authentication for internal users from within</td>
</tr>
<tr>
<td></td>
<td>the system. Use Access Point to configure external users.</td>
</tr>
<tr>
<td>Provider Name</td>
<td>(Required) Name that distinguishes the type of RADIUS authentication being</td>
</tr>
<tr>
<td></td>
<td>used.</td>
</tr>
<tr>
<td>Host Name / IP Address</td>
<td>(Required) DNS name or IP address of the authentication server.</td>
</tr>
<tr>
<td>Shared Secret</td>
<td>(Required) Secret for communicating with the server. The value must be</td>
</tr>
<tr>
<td></td>
<td>identical to the server configured value.</td>
</tr>
<tr>
<td>Authentication Port</td>
<td>UDP port configured to send or receive authentication traffic. Default is</td>
</tr>
<tr>
<td></td>
<td>1812.</td>
</tr>
<tr>
<td>Accounting Port</td>
<td>UDP port configured to send or receive accounting traffic. Default is 1813.</td>
</tr>
<tr>
<td>Mechanism</td>
<td>Select the RADIUS authentication protocol: PAP, CHAP, MS-CHAPv1, or MS-</td>
</tr>
<tr>
<td></td>
<td>CHAPv2.</td>
</tr>
<tr>
<td>Server Timeout</td>
<td>Number of seconds to wait for a response from the RADIUS server. Default is</td>
</tr>
<tr>
<td></td>
<td>five seconds.</td>
</tr>
<tr>
<td>Max number of retries</td>
<td>Maximum number of times to retry failed requests. Default is three tries.</td>
</tr>
<tr>
<td>Realm Prefix</td>
<td>Name and delimiter of realm to be prepended to the username during</td>
</tr>
<tr>
<td></td>
<td>authentication.</td>
</tr>
<tr>
<td>Realm Suffix</td>
<td>Name and delimiter of realm to be appended to the username during</td>
</tr>
<tr>
<td></td>
<td>authentication.</td>
</tr>
<tr>
<td>Auxiliary Server</td>
<td>Default is NO. If set to YES, specify a secondary RADIUS server to be used</td>
</tr>
<tr>
<td></td>
<td>when the primary server is not responding.</td>
</tr>
</tbody>
</table>

3 Click Save

4 Enter your username and passcode in the Test Authentication dialog box, then click Test.

   If authentication is successful, users attempting to authenticate with the tenant portals will see a dialog box asking them to log in with their RADIUS credentials, followed by their domain credentials.

5 If the Test Authentication credentials fail, the settings are not saved. Correct the username or passcode and try again.

### Set Up Authentication with RSA SecurID

You can use RSA SecurID to enable 2 Factor Authentication for end users.

**Procedure**

1 Select Settings > 2 Factor Auth.
2 Configure the authentication.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2nd factor Auth Method</td>
<td>Select RSA SecurID</td>
</tr>
<tr>
<td>Maintain Username</td>
<td>Select Yes to maintain the Username during authentication. The user attempting to authenticate must have the same username credentials for RSA and Domain Challenge. If you select No, the username is not locked and the user can enter a different name.</td>
</tr>
<tr>
<td>External Connections Only</td>
<td>If YES, users inside the network do not need to enter RSA credentials. The distinction between internal and external is configured by the service provider. If NO, all users, both inside and outside of the network, must enter RSA credentials.</td>
</tr>
<tr>
<td>Upload Configuration File</td>
<td>Click Select and navigate to the file named sdconf.rec. Click Open.</td>
</tr>
</tbody>
</table>

3 Click **Save**.

### Identity Management

On the Identity Management page, you can add, edit, and configure Identity Manager providers.

The Identity Management page displays currently configured Identity Manager providers, including the following information for each:

- **Status** - Current status of Identity Manager. Hover on icon to view status.
- **Identity Manager URL** - URL of the Identity Manager.
- **Timeout SSO Token** - Timeout value in minutes.
- **Data Center** - Name of data center.
- **Tenant Address** - Address of the tenant appliance.

To add a new Identity Manager:

1 Click **New**.

2 Enter information as described below.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VMware Identity Manager URL</td>
<td>URL of the Identity Manager.</td>
</tr>
<tr>
<td>Timeout SSO Token</td>
<td>Timeout value in minutes.</td>
</tr>
<tr>
<td>Data Center</td>
<td>Name of data center. Select from drop-down list.</td>
</tr>
<tr>
<td>Tenant Address</td>
<td>Address of the tenant appliance.</td>
</tr>
</tbody>
</table>

3 Click **Save**.

To edit an existing Identity Manager:

1 Select the Identity Manager in list.

2 Click **Edit**.
3 Edit information as described below.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Timeout SSO Token</td>
<td>Timeout value in minutes.</td>
</tr>
<tr>
<td>Tenant Address</td>
<td>Address of the tenant appliance.</td>
</tr>
</tbody>
</table>

4 Click **Save**.

To remove an Identity Manager:

1 Select the Identity Manager in list.
2 Click **Remove**.
3 Click **Delete** to confirm.

To configure Identity Management:

1 Click **Configure**.
2 Edit settings as described below.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Force Remote Users to Identity Manager</td>
<td>Select YES to block remote user access except through IDM. Option only displays if Identity Manager status is green.</td>
</tr>
<tr>
<td>Force Internal Users to Identity Manager</td>
<td>Select YES to block internal user access except through IDM. Option only displays if Identity Manager status is green.</td>
</tr>
</tbody>
</table>

3 Click **Save**.
Desktop Connections

This section provides information on setting up and maintaining connections to desktop virtual machines.

This chapter includes the following topics:

- Desktop Protocols
- Using the VMware Horizon Client

Desktop Protocols

There are a variety of connection protocols for establishing connections to desktop virtual machines.

The VMware Horizon Agent has a very small footprint (90Kb) and supports the full Horizon Client capabilities: Blast Extreme, Blast with HTML Access, PCoIP, RDP, HTTPS, SSL, SSO, USB Redirection, printer support, and session management.

The Horizon Agent supports two desktop connection styles: Native Application (Blast Extreme and PCOIP protocols) and HTML Access (Blast with HTML Access protocol).

Blast Extreme

Blast Extreme is a high performance display protocol. The protocol contains both WAN optimization and support for 3D graphics, resulting in a far superior end user experience when compared to RDP.

To use the Blast Extreme protocol:

- Each virtual desktop must have the latest versions of the Horizon Agent and DaaS Agent installed.
- End users must have the VMware Horizon Client installed on their end point device.
- Blast Extreme is the default protocol for Native Clients in the pool settings.

Blast with HTML Access

Blast with HTML Access enables access to a desktop via any HTML5 compliant web browser.

To use Blast with HTML Access:

- Each virtual desktop must have the latest versions of the Horizon Agent and DaaS Agent installed.
- For internal access not via Access Point, SSL certificate install automation must be configured. See Automating SSL Certificate Install for VMware Blast.
There are additional requirements for launching remote applications, as described below.

**System Requirements for Using HTML Access (Blast)**

**Browser on client system:**
- Chrome 41, 42, and 43
- Internet Explorer 10 and 11
- Safari 7 and 8 (Mobile Safari is not supported for this release.)
- Firefox 36, 37, and 38

**Client operating systems:**
- Windows 7 SP1 (32- or 64-bit)
- Windows 8.x Desktop (32- or 64-bit)
- Windows 10 desktop (32- or 64-bit)
- Mac OS X Mavericks (10.9)
- Mac OS X Yosemite (10.10)
- Chrome OS 28.x or later

**HTML Access (Blast) Support for RDSH Applications**

Launching RDSH applications is supported in HTML Access.

Note the following:
- Access Point 2.0 remote access gateway must be deployed (confirm with your Service Provider).
- This functionality does not work for iOS or Android.

**Automating SSL Certificate Install for VMware Blast**

The process described in this appendix is needed to facilitate internal access that is not via Access Point. If you do not have users requiring this type of access, you do not need to perform this procedure.

Note the following:
- You must follow this process on the image before converting the VM to an image or republishing.
- You must repeat this process each time you open and republish an image.

You can install the certificate using post sysprep script execution in order to avoid sysprep issues and duplicate certificate problems. You can also use your own standard practice as well (for example, Active Directory GPO and scripts). See the Horizon View feature pack documentation for SSL certificate requirements.

Follow the steps below to configure post sysprep commands/scripts in the Horizon DaaS environment.
- Import certificate on test machine and note certificate thumbprint.
- Create post sysprep script/batch file on template VM and copy certificate.
- Convert template VM to image or republish.

**Import Certificate and Record Certificate Thumbprint**

The first step in automating SSL certificate install is importing the certificate and recording the thumbprint.

**Procedure**

1. Add the certificate snap-in to MMC by performing the steps below.

   In order to add certificates to the Windows certificate store, you must first add the certificate snap-in to the Microsoft Management Console (MMC). Before you begin, verify that the MMC and certificate snap-in are available on the Windows guest operating system.

   a. On the desktop, click **Start** and type `mmc.exe`.
   b. In the MMC window, select **File > Add/Remove Snap-in**.
   c. In the Add or Remove Snap-ins window, select **Certificates** and click **Add**.
   d. In the Certificates snap-in window, select Computer account, click **Next**, select local computer, and click **Finish**.
   e. In the Add or Remove snap-in window, click **OK**.

2. Import a certificate for the HTML Access Agent into the Windows Certificate Store by performing the steps below.

   To replace a default HTML Access Agent certificate with a CA-signed certificate, you must import the CA-signed certificate into the Windows local computer certificate store. Before you begin, verify that the HTML Access Agent is installed, the CA-signed certificate was copied to the desktop, and the certificate snap-in was added to MMC (see Step 1 above).

   a. In the MMC window, expand the Certificates (Local Computer) node and select the Personal folder.
   b. In the Actions pane, select **More Actions > All Tasks > Import**.
   c. In the Certificate Import wizard, click **Next** and browse to the location where the certificate is stored.
   d. Select the certificate file and click **Open**.
      
      To display your certificate file type, you can select its file format from the File name drop-down menu.
   e. Type the password for the private key that is included in the certificate file.
   f. Select **Mark this key as exportable**.
   g. Select **Include all extendable properties**.
h Click **Next** and click **Finish**.

The new certificate appears in the Certificates (Local Computer) > Personal > Certificates folder.

i Verify that the new certificate contains a private key.

1. In the Certificates (Local Computer) > Personal > Certificates folder, double-click the new certificate.

2. In the General tab of the Certificate Information dialog box, verify that the following statement appears: 'You have a private key that corresponds to this certificate'.

3 Import root and intermediate certificates for the HTML Access Agent.

If the root certificate and intermediate certificates in the certificate chain are not imported with the SSL certificate that you imported for the HTML Access Agent, you must import these certificates into the Windows local computer certificate store.

a In the MMC console, expand the Certificates (Local Computer) node and go to the Trusted Root Certification Authorities > Certificates folder.

- If your root certificate is in this folder, and there are no intermediate certificates in your certificate chain, skip this procedure.

- If your root certificate is not in this folder, proceed to step b.

b Right-click the **Trusted Root Certification Authorities > Certificates** folder and click **All Tasks > Import**.

c In the Certificate Import wizard, click **Next** and browse to the location where the root CA certificate is stored.

d Select the root CA certificate file and click **Open**.

e Click **Next**, click **Next**, and click **Finish**.

f If your server certificate was signed by an intermediate CA, import all intermediate certificates in the certificate chain into the Windows local computer certificate store.

1. Go to the Certificates (Local Computer) > Intermediate Certification Authorities > Certificates folder.

2. Repeat steps c through f for each intermediate certificate that must be imported.

4 In the certificate MMC window, navigate to the Certificates (Local Computer) > Personal > Certificates folder.

5 Double-click the CA-signed certificate that you imported into the Windows certificate store.

6 In the Certificates dialog box, click the **Details** tab, scroll down, and select the Thumbprint icon.

7 Copy the selected thumbprint to a text file.

   For example:
Note When you copy the thumbprint, do not include the leading space. If you inadvertently paste the leading space with the thumbprint into the registry key (in Step 7), the certificate might not be configured successfully. This problem can occur even though the leading space is not displayed in the registry value text box.

Create Post Sysprep Script/Batch File and Copy Certificate

The second step in automating SSL certificate install is creating the post sysprep script/batch file and copying the certificate.

Use post build configuration script "SetupComplete.cmd" to import the SSL certificate and configure the VMware HTML Access registry (applies to Windows 7 and later).


For example:

- Copy the SSL certificate file under C: drive. For this example, the "C:\desktone_ca_cert" file.
- Create a file SetupComplete.cmd under "%WINDIR%\Setup\Scripts\" folder. Create "Scripts" folder if it does not exist.
- Add following commands in SetupComplete.cmd file. The thumbprint value is what you copied above.
- Note that if you have root certificate and intermediate certificates in the certificate chain, then you need to add appropriate CertUtil commands in batch file.

```bash
CertUtil -importPFX -f -p "<password>" "C:\desktone_ca_cert.pfx"
reg add "HKLM\SOFTWARE\VMware, Inc.\VMware Blast\Config" /f /v "SslHash" /t REG_SZ /d "31 2a 32 50 1a 0b 34 b1 65 46 13 a8 0a 5e f7 43 6e a9 2c 3e"
del /F /Q "C:\desktone_ca_cert.pfx"
del /F /Q "%systemroot%\setup\scripts\SetupComplete.cmd"
```

- Save the SetupComplete.cmd file. You can test the SetupComplete.cmd file on test machine.

Convert Template VM to Image or Republish

The third step in automating SSL certificate install is converting the template VM to an image or republishing

Procedure

1. Convert the template VM to an image or republish, and create an assignment.

2. Verify the HTML Access connection for the certificate, or check certificates and HTML Access registry on desktops.

Note If the HTML Access (Blast) service generates the self-signed certificate even after you set the valid CA certificate as described above, then you can troubleshoot this issue by looking at the logs located here: %ProgramData%\VMWare\Vmware Blast\Blast-worker.txt
PCoIP

PCoIP is a legacy high performance display protocol.

The PCoIP protocol contains both WAN optimization and support for 3D graphics, resulting in a far superior end user experience when compared to RDP.

To use the PCoIP protocol:

- Each virtual desktop must have the latest versions of the Horizon Agent and DaaS Agent installed.
- End users must have the VMware Horizon Client installed on their end point device.

Using the VMware Horizon Client

This section describes some of the Horizon Client features you should understand and any environment characteristics unique to the DaaS integration. For complete information on using the Horizon Client, refer to the Horizon Client documentation on VMware.com.

Horizon Client Download Link in the Desktop Portal

If necessary, you can download the Horizon Client from the Desktop Portal.

If a user launches the DaaS User Portal and then attempts to connect to a desktop using the Blast Extreme or PCoIP protocol, the Horizon Client is launched and the user is seamlessly signed in. The first time a user launches a PCoIP connection from the Desktop Portal a dialog displays containing a link for downloading the Horizon Client.

If you launch the DaaS User Portal and then attempt to connect to a desktop using the HTML Access (Blast) protocol, you are informed that you need to download the Horizon Client by clicking the link in the information dialog. First enable pop-ups in your browser, then initiate an HTML Access connection.

Accessing Desktops and Applications

Note the following when launching desktops and remote applications.

- If you log into the Horizon Client and have an active application session, you may be prompted to reconnect depending on the Horizon Client settings. The Horizon Client will only prompt to reconnect to an application session once. It will not prompt again until you logout and log back in. If the session fails to connect, users should attempt to launch applications normally.
- You cannot have an active RDS desktop and active remote application session at the same time.
- Idle timeouts are based on the activity on the endpoint device, not on the desktop or application.
- RDP is not a compatible protocol if you are logged in via PCoIP on another device. You must log out of the PCoIP session before attempting to connect via RDP.
- The Horizon Client displays RDS desktops and remote applications as launchable items. If you do not see an option to connect to your RDS pool as a desktop, confirm that the RDSH service is enabled for full desktop access and that you have Horizon Client 3.0 or higher.
The remote application name displayed is the name assigned in the pool, so it is important to make the names meaningful in order to distinguish between the applications when multiple pools are mapped to them.

- The Reset Application function will log you off of all application sessions regardless of the session host you are using.
- USB re-direction is not supported for RDS-based servers.
- Launching RDSH applications is supported in HTML Access. See Blast with HTML Access.

Accessing Local Files with Remote Applications Using File Redirection

The file redirection feature allows users to open local files in entitled remote applications that support given file type.

The feature is enabled in the Horizon Client when the Open local files in hosted applications option is selected.

This functionality allows users to do the following:

- Open a local file in a remote application by double-clicking the file in the client machine or by right-clicking, selecting Open with, and choosing the remote application in the menu.
- In the remote application, browse the complete folder where the file resides.
- Save changes made using the remote application to the local client disk.
- Register an entitled application as a file handler for the file types that those applications can open, or chose to open with the remote application a single time.

When an application has been set as the default handler:

- the file's preview icon will be the entitled application's icon in the application launcher page.
- the file type description will be overridden by the remote application, if any.
- double-clicking a file of that type will launch the View Client.

Session Timeout

The session begins when the user authenticates. This timeout can be changed in the administration console.

- User Activity Heartbeat interval

  This value controls the interval between Horizon Client heartbeats. These heartbeats report to the Tenant the amount of idle time that has passed. Idle time occurs when there is no interaction with the end point device, as opposed to idle time in the desktop session. In large desktop deployments, it may reduce network traffic and increase performance to have the activity heartbeats at longer intervals.

- User Idle timeout
This value controls the maximum time that a user can be idle while connected to the Tenant. When this time is reached, the user is disconnected from all active Horizon Client Desktop sessions. Additionally, when the user returns, they will be required to re-authenticate in order to access the Horizon Client.

**Note**  The User Idle timeout should always be greater than the User Activity Heartbeat interval, and is recommended to be at least double the User Activity Heartbeat Interval to avoid unexpected disconnects from desktops.

### Broker Session timeout

This value controls the maximum time that a Horizon Client can be connected to the Tenant before its authentication expires (timeout count starts each time you authenticate). When this timeout occurs, you will not be automatically disconnected from the desktop and are able to keep working, but if you then perform an action that causes communication to the broker (for example, changing settings), the system requires you to re-authenticate and also to log back into the desktop.

**Note**  The Broker Session timeout should always be greater than the User Idle timeout, and is recommended to be at least equal to the sum of the User Activity Heartbeat interval and the User Idle timeout.

**Note**  Horizon Clients running on the Android OS have been known to override this policy setting, resulting in a session timeout of approximately ten minutes.

### Resetting the User Password

When logging in to the Horizon Client, a user might be prompted to change their password.

- After entering the new password, the Horizon Client displays a message indicating that the password reset was successful. However, the password is not actually updated until the connection to the Horizon Agent has occurred. So if the session times out before the connection occurs or the user never launches a desktop session, the password will not be updated.

- If the new password does not conform to AD rules, the log in will be unsuccessful. The user then needs to exit the Horizon Client and attempt to reset the password again. Note that the following character combinations cannot be used in Horizon Client passwords:

  `<`

  `>`

  `<!—`

  `&amp;`

### Desktop Options

After logging into a desktop, a user can click Options to open the Options menu. The following table describes the functionality available from the Options menu.
<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Switch Desktop</strong></td>
<td>Allows the User to access the Desktop Selection Screen or Switch between open desktop sections. See the Desktop Selection Screen Section for controls and info. This will not work if your session has timed out.</td>
</tr>
</tbody>
</table>
| **Autoconnect to this Desktop**| For PC and thin clients, makes the specified desktop the user's default desktop when the desktop is part of a dynamic pool. On the next login, the desktop will immediately be displayed as long as:  
  - The user has only one desktop mapped to them.  
  - There is not a problem with the login credentials or desktop state.  
  If a user selects Autoconnect and then logs in with multiple desktops, the Autoconnect to this Desktop setting is set to off/false. If the session times out, the Autoconnect setting is not saved and the user cannot autoconnect at the next log in. |
| **Reset Desktop**              | Triggers a reboot on the desktop. This will not work if the session has timed out. |
| **Disconnect**                 | Disconnects the current user from their active session. |
| **Disconnect and Logoff**      | Disconnects and logs off the user from their active session. |

**Triggering a Desktop Logoff**

Logging off initiates a call to the DaaS Agent, which can take up to 30 seconds to complete. As a result, if a user attempts to log back in before the 30 seconds elapses, the log off dialog might still be present.

**VRAM Settings During Assignment Provisioning**

To prevent black screen, the platform provisions assignments of these desktops with the video RAM (VRAM) size set to 128. This setting can be changed by your service provider.
Troubleshooting

This section describes the most common problems you might need to troubleshoot.

For information on other problems that might occur when using VMware software, refer to the VMware Knowledge Base.

This chapter includes the following topics:

- Troubleshooting Horizon Client Connections
- Troubleshooting HTML Access (Blast) Connections
- Black Screen
- Overriding ADM PCoIP Defaults
- Error Messages
- Emergency Direct Desktop Connection Without Tenant
- Give Feedback Menu Choice Does Not Work

**Troubleshooting Horizon Client Connections**

There are several configuration/setup problems that can result in an inability to use the Horizon Client successfully

<table>
<thead>
<tr>
<th>Problem</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Login Problems</td>
<td>If you cannot log in to the Horizon Client, verify that the version of the VMware Horizon Client you are using is compatible with VMware View 5.1 or higher.</td>
</tr>
<tr>
<td>Desktop Does Not Launch</td>
<td>If the Desktop does not launch, verify that no other software in the environment is using port 443.</td>
</tr>
<tr>
<td>Unable to Connect to Desktop</td>
<td>If you receive the error message “Unable to Connect to Desktop,” it means that the View Agent is not running. In the Windows Control Panel programs, verify that Horizon Agent and View Agent Direct Connect appear in the list of installed programs. If they do not, the installation did not complete properly and you will need to reinstall. If the View Agent software is installed, verify that the View Agent Service is running.</td>
</tr>
</tbody>
</table>
**Problem** | **Solution**
--- | ---
Desktop Disconnects | If a Horizon Client session ends too quickly when idle, this means that Horizon Client Session Timeout settings are configured to allow only a very short idle period. You can configure the Horizon Client Session Timeout settings in the administration console.

**Black Screen** | See Black Screen.

---

## Troubleshooting HTML Access (Blast) Connections

There are several configuration/setup problems that can result in an inability to launch a HTML Access (Blast) connection successfully.

<table>
<thead>
<tr>
<th>Problem</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Browser is not HTML5 compliant</td>
<td>Check that the browser version is one cited in the requirements.</td>
</tr>
<tr>
<td>Pop-up blocker enabled</td>
<td>The browser's pop-up blocker could prevent opening the new window for a HTML Access connection. Make sure that the user disables the pop-up blocker for the Desktop Portal.</td>
</tr>
<tr>
<td>Windows firewall disabled</td>
<td>Make sure that the Windows Firewall is installed and running on the user's desktop. A disabled Windows Firewall will result in errors reported in the HTML Access logs.</td>
</tr>
</tbody>
</table>

## Black Screen

Users can see a black screen for a variety of reasons.

- When you update VMware Tools, the update can in some cases install the wrong video driver, resulting in black screen. The workaround is to log into the session using RDP and install the correct driver.
- If the System Administrator moves a desktop from a non-PCoIP pool to a PCoIP pool and users experience a black screen when trying to connect to the desktop, solutions can be found in the VMware Knowledge Base.
  - Refer to the steps outlined in the VMware Knowledge Base article Black screen when logging into a VMware View virtual desktop using PCoIP.
  - Verify that the Video RAM (VRAM) settings in the Virtual Machine settings (.vmx) file are set properly for multi-monitor access when using the PCoIP protocol. Refer to the VMware Knowledge Base article Determining display and screen resolution settings for PCoIP.
  - Verify that the Video driver is correct for the VMware View Agent and operating system. Refer to the VMware Knowledge Base article "The PCoIP server log reports the error: Error attaching to SVGADevTap, error 4000: EscapeFailed."

## Overriding ADM PCoIP Defaults

ADM can be configured on the Domain Controller or the master desktop image being used to create a gold pattern.
On the master desktop image, the System Administrator can override ADM defaults by running gpedit.msc on the desktop and navigating to the Administrative Template > Classic Administrative Templates (ADM) > PCoIP folder.

**Error Messages**

This sections describes error messages that users can encounter during desktop connections.

- **Error 500**

  If a user receives Error 500 in the Horizon Client, look in the tenant log and make a note of the exception before contacting support. The exception to look for will mention the ViewClientServlet.

- **Common Error Messages**

  The following table lists the most common error messages users can receive and the causes when using the Horizon Client to connect to their desktop. The Error Details portion of the message provides information needed by customer support to troubleshoot the connection problem.

<table>
<thead>
<tr>
<th>Error Message</th>
<th>Error Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>View Agent Login Failed. Error Details: &lt;Message from Agent&gt;</td>
<td>The View Agent failed the login request sent.</td>
</tr>
<tr>
<td>Session has Expired, Please Restart Horizon Client to Connect</td>
<td>Desktop Portal session timeout has occurred. The Desktop Portal timeout is based on a policy (userportal.session.timeout) set at the service provider, but may be overridden by a setting in the administration console.</td>
</tr>
<tr>
<td>Unable to allocate a desktop - pool refresh is in progress.</td>
<td>Wait a few minutes and try again. Dynamic pool refresh is underway. This means that desktops are being destroyed and recreated based on a new or altered Gold Pattern. Once the refresh completes, users will be able to log into their desktop.</td>
</tr>
<tr>
<td>Error communicating with desktop. Please contact your Administrator. Error Details: Desktop Agent Communication Error</td>
<td>Unable to parse error from Authentication Error Response due to interrupted communication between the Horizon Client, Tenant and View Agent Connect. There might be a warning or error in the desktop.log file related to ViewClientServlet.</td>
</tr>
<tr>
<td>Could not parse XML</td>
<td>Data Horizon Client or Agent returned XML which could not be read by the DaaS platform.</td>
</tr>
<tr>
<td>Desktop is not ready for connection (DaaS Agent may be starting up). Please wait a few minutes or try again. If problem persists, please contact your Administrator.</td>
<td>DaaS Agent is reported as offline. Reboot the desktop if the problem persists and console access is too long. The DaaS Agent should come up when the desktop comes up (within a few minutes).</td>
</tr>
<tr>
<td>Desktop is not ready for connection (may be shutting down or rebooting). Please wait a few minutes or try again. If problem persists, please contact your Administrator.</td>
<td>OS state is not running. Wait until it is running or reboot from Desktop Portal or administration console.</td>
</tr>
<tr>
<td>Desktop is not ready for connection (currently in maintenance mode). Please wait a few minutes or try again. If problem persists, please contact your Administrator.</td>
<td>Domain rejoin maintenance is occurring for a dynamic desktop. This can also occur during dynamic pool refresh.</td>
</tr>
<tr>
<td>Error Message</td>
<td>Possible Solution</td>
</tr>
<tr>
<td>------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Unable to Connect to Desktop. Please contact your Administrator. Error Details: View Agent is not running</td>
<td>The DaaS Agent has reported that the View Agent service is not running or listening on the require ports. Make sure that the View Agent is installed and that the firewall ports are open (4172, 32111, 443). Reboot machine or check service &quot;View Agent Connect&quot; through RDP (User Portal) if possible.</td>
</tr>
<tr>
<td>Unable to Connect to Desktop. Please contact your Administrator. Error Details: VMware Tools is not running</td>
<td>VMware Tools are offline. See troubleshooting/solution on VMware tools.</td>
</tr>
<tr>
<td>Unable to Connect to Desktop. Please contact your Administrator. Error Details: VMware Tools is not installed</td>
<td>VMware Tools are not installed. See troubleshooting/solution on VMware tools.</td>
</tr>
<tr>
<td>Unable to Connect to Desktop. Please wait a few minutes and try again. If problem persists, please contact your Administrator</td>
<td>Desktop Unavailable. This is a generic message from the Allocator Service. Try checking the state of the machine and the tenant system to see if there are other issues.</td>
</tr>
<tr>
<td>Unable to Connect to Desktop. Desktop has been allocated to a different user. Please Contact your Administrator. Error Details: Desktop Already in Allocated State.</td>
<td>Another user has been allocated this desktop. A session exists with a GUID different from the current user.</td>
</tr>
<tr>
<td>Login Failure. Please contact your Administrator. Error Details: Unable to lookup user GUID using credentials</td>
<td>An exception was raised by the Horizon DaaS software during a GUID lookup. Possible reasons include: Domain controller is offline; the Fabric node had failures; general tenant problems.</td>
</tr>
<tr>
<td>Unable to Connect to Desktop. Please wait a few minutes and try again. If problem persists, please contact your Administrator. Error Details: Unknown IP Address</td>
<td>IP Address is null or invalid. The IP address can be null if the DaaS Agent is in the middle of logging in or the VM is starting up.</td>
</tr>
<tr>
<td>Unable to Connect to Desktop. Please contact your Administrator. Error Details: Invalid IP Address &lt;IP_address&gt;</td>
<td>The IP address is listed only if it is known.</td>
</tr>
<tr>
<td>Unable to Connect to Desktop. Please contact your Administrator. Error Details: Unable to retrieve Tenant Domain information</td>
<td>There is no Domain information logged in the database. The DaaS platform cannot associate the tenant with any Domain.</td>
</tr>
<tr>
<td>Login Failure: Unknown user name or bad password. Please try again.</td>
<td>User name or password are invalid for the given domain.</td>
</tr>
<tr>
<td>Unable to Allocate Desktop, No Desktops Available. All desktops in pool are currently in use.</td>
<td>Dynamic pool has no desktops that are available to the user.</td>
</tr>
<tr>
<td>Unable to Connect to Desktop (current connected protocol incompatible). Please log off previous session and try again.</td>
<td>The Allocator Service is indicating the current session is using a non-compatible protocol.</td>
</tr>
<tr>
<td>Unable to complete log off. If problem persists, please contact your Administrator. Error Details: Invalid session id</td>
<td>This error occurs if the DaaS platform cannot parse the XML, the session-id key returned in the XML is null, or if the key is malformed.</td>
</tr>
<tr>
<td>Unable to complete log off. If problem persists, please contact your Administrator. Error Details: Unable to Associate Session Id with Active Sessions</td>
<td>There are no active sessions for the current user.</td>
</tr>
</tbody>
</table>
Unable to complete log off. If problem persists, please contact your Administrator. Error Details: Error communicating with Desktop Manager

The desktop <x>,<n> is not in the list of entitled desktops

In this message, <x> is the application name you are attempting to launch and <n> is a number.

This message indicates that you may be using an incompatible Horizon Client and should reference the client’s release notes to confirm it supports Remote Application functionality.

- Error Messages Associated with Password Changes

The following table lists the error messages a user can receive and the causes when attempting to change their password in the Horizon Client.

<table>
<thead>
<tr>
<th>Error Message</th>
<th>Cause</th>
</tr>
</thead>
<tbody>
<tr>
<td>Please Enter the Old Password and the New Password.</td>
<td>Some or all of the password fields are blank.</td>
</tr>
<tr>
<td>Provided Old Password is invalid, please try again.</td>
<td>If the password you logged in with is different from the &quot;Old Password&quot;.</td>
</tr>
<tr>
<td>Provided New Passwords do not match, please try again.</td>
<td>The user mistyped the password.</td>
</tr>
<tr>
<td>Please Enter a New Password that is different from the Old Password.</td>
<td>The new password the user entered is the same as their old password</td>
</tr>
<tr>
<td>Unable to Change Password. Please restart Horizon Client and try again.</td>
<td>After the user selected desktop, completing password change screen, and clicked connect, the View Agent was unable to change the Domain password.</td>
</tr>
</tbody>
</table>

Note

A user confirmation dialog after the password change screen incorrectly indicates "You successfully changed your password and should use it in the future."

- Note that the following character combinations cannot be used in Horizon Client passwords:
  
  `<`
  
  `>`
  
  `<!—`
  
  `&`

  For example, none of the following passwords are supported:

  Deskton
  
  `< Deskton>`
  
  Deskton `<!—`
  
  Deskton`&`;
Emergency Direct Desktop Connection Without Tenant

In an emergency situation where a tenant is down or unreachable but the network is still working, you can globally instruct all DaaS Agents to allow temporary RDP native access so end users can connect without the broker being functional.

To enable this temporary functionality, add the registry keys described below to the desktop VMs, either directly or via GPO policy. Add the keys in one of the following locations, depending on whether the DaaS Agent is installed on a 32-bit or 64-bit Windows system:

- HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.\VMware DaaS Agent (32bit)
- HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\VMware, Inc.\VMware DaaS Agent (64bit)

<table>
<thead>
<tr>
<th>Key</th>
<th>Type</th>
<th>Value</th>
</tr>
</thead>
</table>
| AllowDirectConnections     | DWORD | 0 = do not allow direct connections  
1 = allow direct connections. |
| DirectConnectionExpiryInUTC| REG_SZ| Date and time until which direct connections are allowed if direct connections access is enabled (AllowDirectConnections = 1).  
Date and Time Format: YYYY-MM-DD HH:MM:SS |

This functionality requires the following:

- DaaS Agent 17.2 is in use.
- RDP access is not being blocked via View or any other GPOs.
- The user is in a group associated with a desktop assignment. The DaaS Agent configures the same users/groups for RDP access in the desktop (local RDP group).

**Note** The default Group Policy refresh interval is 90 minutes. You have to perform additional steps to force a refresh sooner than that. See the relevant Microsoft documentation for more information.

Give Feedback Menu Choice Does Not Work

When you click the **Give Feedback** menu choice in the Administration Console, nothing happens or a browser error message appears.

**Problem**

The Administration Console's Help menu ( помощь) has a **Give Feedback** choice. Depending on your settings for your local system's browser or mail application, when you click it, you might see one of the following:

- Nothing happens.
- A browser error message appears.
Cause

The design for this menu choice is to run the new mail action of your local system's default mail application, using mailto:feedback.horizonair@vmware.com. This error occurs when the browser cannot perform the mailto action, such as under these conditions:

- Your browser is set up to block pop-up windows.
- Your browser's applications list is not configured with a default action for the mailto content type or the mailto content type is configured with the action Always ask.
- Your local system does not have a default local mail application configured.

Solution

1. If your browser blocks pop-up windows, add the Administration Console's URL to the exception list.
2. Configure your browser's mailto content type's action with a mail application, so that the Give Feedback choice can successfully open a new email form.
3. If you do not want to change your browser settings, you can submit feedback by manually sending an email to feedback.horizonair@vmware.com.
The following are technical notes regarding various system features.

- **Custom Branding**
  
  If you have a custom branding scheme for the Desktop Portal, you will need to check whether everything appears as expected after upgrading a tenant. There are a few areas to which you should pay particular attention due to VMware branding changes.
  
  - Login page:
    
    CSS selector: `#productNameInner`
    
    You may need to adjust the margin-left property and/or decrease the font-size, for example:
    
    ```
    font-size: 14px;
    ```
  
  - Other pages:
    
    You will likely need to make the same changes as for the login page. Additionally, you may need to adjust the background-position of the `#banner` selector:
    
    ```
    background-position: 0px 0px;
    ```

- **Enabling Post-Sysprep Commands**
  
  To enable post-sysprep commands, perform these steps on a desktop before converting it to an image.
  
  1. Create a folder named `sysprep` under `C:\driver`.
  2. Create a batch file named `postprep-extra.bat` in the `sysprep` folder.
  3. Add required commands in batch file and save it.
  4. Convert the desktop to an image. File path: `c:\sysprep\postprep-extra.bat`. Sysprep launches this batch file during specialize pass execution (before agent comes and joins the domain).

  To set the post sysprep batch file in the template before converting to a gold pattern (executed before domain join), perform the following steps.
  
  1. Create a batch: `c:\sysprep\postprep-extra.bat`
  2. Create the `C:\Sysprep\...` folder structure (for Windows 7): `C:\Sysprep\ postprep-extra.bat`
  3. Save it with your commands. Sysprep executes this batch file in post execution.
Helpdesk Console (Beta Feature)

The Helpdesk Console is a user interface that you can use to access VMs, perform health scans, get remote assistance, and perform other tasks.

Notice Regarding Beta Features and Support

HELPDESK CONSOLE IS PROVIDED "AS IS", WITHOUT SLA OR WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

If you encounter questions or issues using Helpdesk Console, you can send them to deployment@vmware.com. VMware is not committed to productization of any features or resolution of any issues of the Helpdesk Console.

This chapter includes the following topics:
- Access the Helpdesk Console
- Launch a Console for a Virtual Machine
- Set Up a Health Scan
- Get Remote Assistance
- View Usage Report
- Image Upload
- View History

Access the Helpdesk Console

You can access the Helpdesk Console from your web browser.

Note the following:
- Use HTTPS, not HTTP. Using HTTP will not launch the console.
- Chrome is the only supported browser for Console access. The following browsers are not yet supported: Microsoft Internet Explorer, Firefox, Safari, and Opera.
If console access is failing to launch, you may need to open the following URL and accept the certificate: https://<tenant_appliance_tenant_network_ip>:18001/

In a vCloud Director based environment, you need to make sure your browser accepts the vCloud Director server certificate.

Access to the Helpdesk Console is restricted to:

- Tenant Administrators (Users with Admin access to the Administration Console)
- Members of the Horizon_Air_Helpdesk AD group. This group can be used to provide access to support personnel that are not tenant administrators.

**Procedure**

1. In a Chrome web browser, navigate to https://<TenantApplianceNodeAddress>/haca where `<TenantApplianceNodeAddress>` is the IP address of the tenant.

   The login page displays.

2. Enter your admin username and password, confirm that the correct domain is selected, and click Login.

   The Virtual Machines tab displays, containing a list of all VMs in all pools.

---

**Launch a Console for a Virtual Machine**

To launch a console for a virtual machine in the Helpdesk Console, click the VM name in the Virtual Machines list.

A console opens showing the login screen for the VM. Ctrl-Alt-Del and power operations are supported by buttons in the top right of the console window.

---

**Set Up a Health Scan**

The Health Scan tool allows you to monitor application of VM changes that may compromise the port access, performance, or overall access by end users to the desktop.

**Procedure**

1. Install the Horizon DaaS Health Agent on all VMs that will be monitored. Click the **Install Horizon DaaS Health Agent** link at the top right of the VM Health Scan tab for more information.

   **Note** By default, the Health Agent listens on TCP port 10762.

2. Filter the list as desired using the Scan Filter field and/or Select Pool drop-down list.

3. Initiate the scan by doing one of the following:
   - Click **One Time Scan** to perform a single scan immediately.
   - Enter a number of minutes and click **Schedule Scan** to schedule recurring scans at a selected time interval.
Information for the scanned VMs appears in columns as described below.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VM</td>
<td>Name of the virtual machine.</td>
</tr>
<tr>
<td>Pool</td>
<td>Pool (assignment) to which the VM belongs.</td>
</tr>
<tr>
<td>IP</td>
<td>IP address of the VM.</td>
</tr>
<tr>
<td>Result</td>
<td>Overall result of the scan. Result can be:</td>
</tr>
<tr>
<td></td>
<td>- Power off – VM is powered off.</td>
</tr>
<tr>
<td></td>
<td>- Agent failure – Health Agent is not installed or reachable on the VM</td>
</tr>
<tr>
<td></td>
<td>- VM issue(s) - Indicated by an &quot;X&quot; icon with number next to it. VM has one/more issues, which are detailed in other columns.</td>
</tr>
<tr>
<td>Ports</td>
<td>Verifies that necessary ports are open.</td>
</tr>
<tr>
<td>Firewall</td>
<td>Indicates whether the VM's firewall is enabled.</td>
</tr>
<tr>
<td>Sleep Policy</td>
<td>Indicates whether there is a policy set on the VM to put it in a sleep state.</td>
</tr>
<tr>
<td>Services</td>
<td>Verifies that the following services are running:</td>
</tr>
<tr>
<td></td>
<td>- Desktop Windows Manager Session Manager</td>
</tr>
<tr>
<td></td>
<td>- VMware HTML Access (Blast)</td>
</tr>
<tr>
<td></td>
<td>- VMware Horizon Agent</td>
</tr>
<tr>
<td></td>
<td>- VMware DaaS Agent</td>
</tr>
<tr>
<td></td>
<td>- VMware Tools</td>
</tr>
<tr>
<td>RDP Enabled</td>
<td>Verifies that RDP is enabled and set to allow connections from computers running any version of RDP.</td>
</tr>
<tr>
<td>BAD IP</td>
<td>Verifies that the desktop does not have a 169.x.x.x IP address, and so is more likely to get DHCP.</td>
</tr>
<tr>
<td>DHCP</td>
<td>Verifies that the desktop is set for DHCP, not STATIC.</td>
</tr>
<tr>
<td>Domain Trust Relationship</td>
<td>Confirms domain trust relationship between desktop and Domain Controller.</td>
</tr>
<tr>
<td>Remote Assistance</td>
<td>Verifies Remote Assistance is enabled on the desktop.</td>
</tr>
</tbody>
</table>

4 When the scan is complete, you can perform the following actions:

- Mouse over the errors in the scan results table to see additional information.
- Click the Report button on the top left of the list (button is labelled Report: <day date time>) to view history of recent scans performed. In this table, double-clicking anywhere in a row opens the results for that scan.
- Select the Show Only VMs with Error check box to hide VMs that have no errors.
- Type a name or partial name in the Search field and press Enter to search for VMs by name.
- Select a value in the Show drop-down menu to adjust number of VMs shown per page.
Click **Export** and select one of the following options:

- **Copy** – Copy information to clipboard.
- **CSV** – Export results in CSV format.
- **PDF** – Export results in PDF format.
- **Print** – Generate a printable web version of the results.

**Get Remote Assistance**

The Remote Assistance tool provides a way for a helpdesk operator or administrator to shadow an active user session.

For more information on using this feature, click the **Guide for Remote Assistance** link on the Remote Assistance tab.

**View Usage Report**

The Usage Report tab displays usage trends and allows you to view user activity session reports.

The Usage Report can be filtered by date, pool, and data type. Data displayed in the Usage Report include:

- Usage Trends – Max Concurrent Users, Max Concurrent Sessions, Daily Unique Users, Total Capacity
- User information – Client Access Demographics, Internal vs. External Users Access
- Session information – Protocol, Service Type, Session Duration

Pool-based usage information such as max concurrent users and unique users accessing a specific pool can be helpful for determining overall utilization and licensing requirements of your applications on RDSH pools.

Select **User Activity** from the Usage Report drop-down menu to view the User Activity Summary.

Click on a user name in the User Activity Summary list to view User Activity Details.

**Image Upload**

The Image Upload feature allows you to upload OS images to use for assignment creation.

You can do this one of two ways:

- If you already have a prepared VM, you can upload the image from its current location.
- You can export a Horizon View desktop pool template using tool hvexport, and then import the prepared template using Image Upload.
Uploading an Image

The process of uploading an existing image consists of the following.

- Prepare image for upload.
- Perform upload steps.
- Troubleshoot upload (if necessary).

Prepare Image for Upload

The Image Upload Service can be used with generic VM templates in OVF format. The VM must be prepared properly before importing.

Procedure

1. Click the Help link to view requirements for desktop software/service.
2. Click the Download Agents link to download required software (agent) and SSL certificate. The files are prepared by your service provider, according to your tenant appliance version.
3. Confirm that the following requirements have been met.
   - **Software**
     You can download required software from the Download Agents link on Image Upload Service page. The following software must be installed:
     - Horizon DaaS Agent
     - Horizon Agent
     - Horizon DaaS Health Agent
   - **SSL Certificate**
     Horizon DaaS tenant certificate file must be configured in DaaS agent. You can download it from the Download Agents link on Image Upload Service page. With default DaaS Agent installation on x64 system, the certificate file must be copied to:
     C:\Program Files (x86)\VMware\VMware DaaS Agent\cert\cacert.pem
   - **Services**
     The following services must be configured as auto start:
     - VMware DaaS Agent (DaaS Agent)
     - VMware Horizon View Agent (WSNM)
     - Windows Firewall (MpsSvc)
     - Desktop Window Manager Session Manager (UxSms)
     - VMware Blast (VMBlast)
4 If you have multiple desktop managers, update desktop manager ip addresses in DaaS agent configuration file. With default DaaS Agent installation on a x64 system, the configure file is:

C:\Program Files (x86)\VMware\VMware DaaS Agent\service\MonitorAgent.ini

- Find the following line:
  ;standby_address=<uncomment and add comma separated standby address list>
- Uncomment the line by removing the semicolon at the beginning, and add desktop manager addresses separated by commas. For example:
  standby_address=192.168.11.3,192.168.11.4,192.168.11.5,192.168.11.6

5 Before performing the export, confirm the following:

- Network adapter type is VMXNET3. E1000 will not work.
- There is no ISO attached to the VM. You can safely remove any virtual CD-ROM drive.
- The target hypervisor supports your virtual machine version. Due to mixed infrastructure, the latest virtual machine might not always be supported. If possible keep your virtual machine version low. For example, version 8. You can contact your service provider for information about supported virtual machine versions, or attempt to use the tool, since it will report an error if the virtual machine version is incompatible.
- No 3D graphic card capability is enabled on the VM.
- The virtual machine is exported as OVF, since OVA is currently not supported by the Image Upload feature.

Upload the Image

After you have prepared the image, you can upload it.

Procedure

1 On the Image Upload tab, click the Choose Files button to choose the virtual machine files.

   Normally this includes the following files:
   - One .ovf file
   - One or more .vmdk files
   - Optionally one .mf file

   Note the following:
   - Do not choose any .iso file. If you see any .iso file, edit your virtual machine, remove all CD-ROM drivers, and export again.
   - Currently OVA file is not supported yet. To convert OVA file to OVF format, rename the OVA file extension ".ova" to ".zip", then use a zip tool to extract the archive. The extracted files are in OVF format.

   The uploaded VM template is converted to a desktop image.
2 After the ovf files are selected, click the Configuration link to bring up the configuration page and fill in proper configuration.

3 Click the Start Import button to launch the import process.

The progress is shown with a detailed message.

**Note** You can deploy the uploaded VM to another datacenter or desktop manager without uploading again. Select the Previously uploaded radio button in the Image Files section to reuse the uploaded files.

**Troubleshoot the Upload**

If the process fails, the failure details will be shown in the lower portion of the Image Upload tab.

- If the virtual machine has not been deployed, then depending on the error reason, you may need to re-upload a new one or attempt to redeploy.

- If the VM has been deployed, but the conversion of gold pattern fails, the VM could appear in the "Imported Desktop" pool, or "Reserved Desktop" in pattern management. Locate the VM there and prepare the image manually using Console Access in the Helpdesk Console and the Administration Console. This allows you to skip re-upload/deploy, which could take a long time if the VM image is large.

**Using a Template From Horizon View**

To use a template from Horizon View, you must do the following.

- Export the template from Horizon View and prepare the image
- Upload the file in the Helpdesk Console

**Export Template From Horizon View and Prepare Image**

The hvexport tool is used to export desktop pool templates from Horizon View.

The tool also helps preparing the image, including checking configuration, downloading proper software and auto-installing and downloading the DaaS certificate and copying it to DaaS agent folder.

**Procedure**

1 Click the Help link on the Image Upload page.

2 Click the links to download the tool and the platform configuration.

   The platform configuration is dynamically generated, and is used by the tool.

3 Extract the downloaded archive.

   The hvexport tool includes three folders (export, repos, and software) and five files:
   - hvexport.bat
   - hvexport.jar
Files are organized as follows:

- Downloaded ImgUploadSvc.conf in the tool folder.
- Required software downloaded automatically (e.g. DaaS agent, View agent) in the software directory.
- The export directory is the default directory where Horizon View desktop pool template will be exported to.

**Note** The tool is a Java application and requires JRE to run.

4. Launch the application using hvexport.bat or .sh. Follow the guide of the tool to export the VM and prepare the OS image.

The tool is interactive, and will eventually create a linked clone of the target template VM on vCenter, and automatically upload required software into the guest OS. The following items are automatically downloaded:

- Horizon DaaS Agent
- Horizon View Agent
- Horizon DaaS Health Agent

In addition, tenant certificate (cacert.pem) is required for preparing the gold pattern. The tool also prepares the certificate, which is contained in the platform configuration file (ImgUploadSvc.conf) previously downloaded.

The uploaded files should be installed automatically. In case something wrong with the image preparation, you can perform it manually on the target desktop.

The hvexport tool performs a validation of the environment after software installation.

The tool also persists state into a file, so it can be started over. Fields previously input will have a default value. For example, connection server address.

5. Press ENTER directly to use the default value.

**Upload the File**

After you have exported the template and prepared the image file, you can upload it in the Helpdesk Console.

After the template is exported, by default it appears in the export directory of the hvexport tool.
Procedure

1. On the Image Upload tab, click Choose File and select all files in the export folder, except for any .iso file that may be present. There should be one .ovf file, one pool.conf file, one or more .vmdk file. Do not upload any iso file.
   If the pool.conf file is a pool exported by hvexport tool, the configuration will be shown automatically, with some fields populated.

2. Click OK to close the dialog.

3. Click the Start Import button.
   The import process completes, with progress indicated on the screen.

View History

The History tab provides the access log for auditing purposes.
You can search or filter data by pool (assignment) using the controls at the top of the page.