Horizon Cloud with On-Premises Infrastructure Administration Guide

VMware Horizon Cloud Service

Horizon Cloud with On-Premises Infrastructure 1.3

vmware®

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

https://docs.vmware.com/

The VMware Web site also provides the latest product updates.

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

docfeedback@vmware.com

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

Contents

About Horizon Cloud with On-Premises Infrastructure Administration

This Horizon Cloud with On-Premises Infrastructure *Administration* document explains how to use the VMware Horizon® Cloud Service® and your Horizon Cloud with On-Premises Infrastructure environment to create, deploy, and administer virtual desktops and applications. This information describes how to use the product after you complete all the tasks outlined in the Horizon Cloud with On-Premises Infrastructure *Installation and Configuration* document.

Intended Audience

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

Depending on your organization's needs, you might find it helpful to be familiar with these VMware software products, software components, and their features:

- VMware vSphere®
- VMware vCenter Server® Appliance™
- VMware ESXi™, the hypervisor
- VMware vSphere® Web Client or VMware vSphere® Client™
- VMware User Environment Manager™
- VMware Unified Access Gateway™
- VMware Identity Manager™

VMware Information Experience Glossary

VMware Information Experience 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.

Contacting VMware Support

Contact VMware Support when you need help with your Horizon Cloud with On-Premises Infrastructure environment.

- You can submit a support request to VMware Support online using your My VMware® account or by phone.
- KB 2144012 *Customer Support Guidelines* provides details for getting support depending on the issue encountered.

- After you have configured your Horizon Cloud Node, you can submit a support request by logging in to the Administration Console and clicking  > **Support**.

Introduction to Horizon Cloud with On-Premises Infrastructure

With a Horizon Cloud with On-Premises Infrastructure environment, end users can securely access their desktops and applications from any device. After you deploy the Horizon Cloud Node, you can use the Administration Console to configure desktop and application assignments.

A Horizon Cloud with On-Premises Infrastructure environment consists of a cloud service, Horizon Cloud, which pairs with an on-premises component called the Horizon Cloud Node.

Horizon Cloud	A control plane hosted in the cloud by VMware for the central orchestration and management of virtual desktops and applications on an on-premises infrastructure.
Horizon Cloud Node	Optimized hardware that is connected to the cloud control plane by way of integrated Horizon Cloud with On-Premises Infrastructure connector software and configured for the Horizon Cloud with On-Premises Infrastructure environment. vSAN Ready Nodes or Dell EMC VxRail appliances are types of optimized hardware you can configure as Horizon Cloud Nodes.

Along with access to the Administration Console, also referred to as the Horizon Cloud Manager, a Horizon Cloud with On-Premises Infrastructure environment includes the software necessary to perform the following tasks.

- Pair the on-premises hardware with the cloud control plane.
- Deliver virtual desktops and manage applications as containers known as AppStacks.

Using User Environment Manager for Persistence

A Horizon Cloud with On-Premises Infrastructure environment uses the VMware next-generation desktop and application delivery platform known as JMP (Just-in-Time Management Platform). JMP is a set of VMware technologies that deliver Just-in-Time desktops and applications. The JMP technologies applicable in a Horizon Cloud with On-Premises Infrastructure environment are:

- VMware Instant Clone Technology, providing fast desktop provisioning for your environment's virtual desktops
- App Volumes, providing real-time application delivery into those desktops
- User Environment Manager, providing contextual policy management

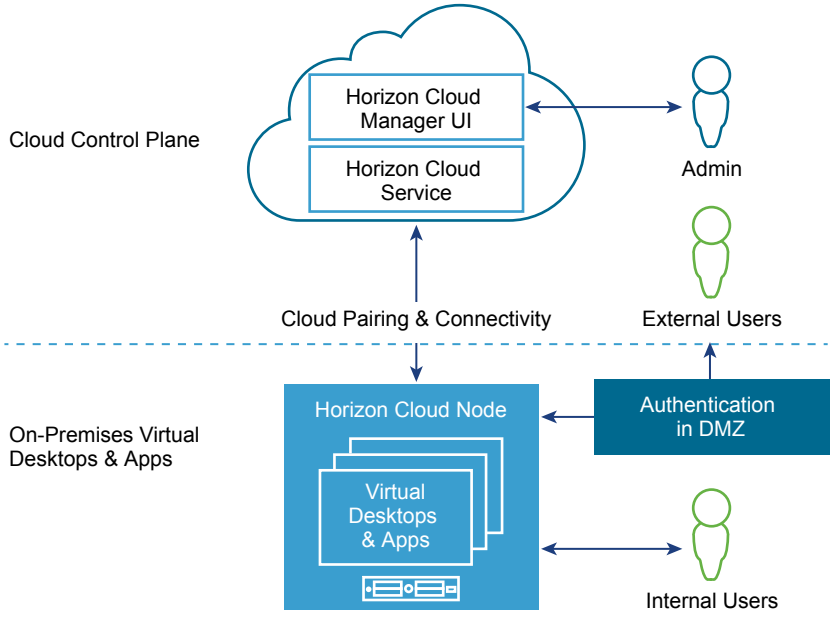
User Environment Manager provides various options for achieving the persistence of end-user data, settings, and profiles of virtual desktops. For a Horizon Cloud with On-Premises Infrastructure environment, the best practice is using User Environment Manager with folder redirection. A pre-defined configuration is available from VMware. For details about this pre-defined configuration along with the best practices for using App Volumes and User Environment Manager with your environment, see the document titled VMware App Volumes with Horizon Cloud Application Delivery Best Practices and Operations Procedures at vmware.com. This document also includes detailed information on the installation and setup of User Environment Manager for use with Horizon Cloud with On-Premises Infrastructure.

Horizon Cloud with On-Premises Infrastructure Architecture

Horizon Cloud with On-Premises Infrastructure consists of a cloud service and on-premises equipment.

Architecture

Horizon Cloud is a control plane that VMware hosts in the cloud. This cloud service enables the central orchestration and management of virtual desktops and applications on an on-premises infrastructure.

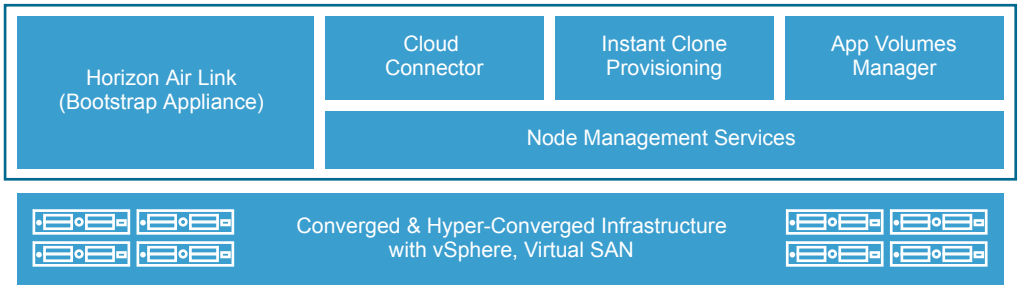


VMware is responsible for hosting the service and providing feature updates and enhancements for a software-as-a-service experience.

The cloud control plane also hosts a common management user interface called Horizon Cloud Manager, also referred to as the Horizon Cloud Administration Console, and Administration Console for short. The Horizon Cloud Manager is accessible from all major browsers and provides IT administrators a single location for managing desktop images, applications, user data, profiles, and assignments. The Horizon Cloud Manager is accessible from anywhere at any time, providing maximum flexibility.

Horizon Cloud Node

A Horizon Cloud Node environment uses a bootstrap appliance named Horizon Air Link to pair with the Horizon Cloud service. You deploy that appliance in your hyper-converged infrastructure. After you deploy the Horizon Air Link appliance, Horizon Air Link orchestrates the initial setup and pairing with the cloud control plane for ongoing management and communication. The Cloud Connector component provides connectivity to the cloud without requiring a dedicated site-to-site VPN.



After the initial pairing is complete, Horizon Air Link begins configuring the supported hyper-converged infrastructure as a Horizon Cloud Node environment. After the Horizon Air Link completes configuring the environment, the following virtual appliances are running in the on-premises infrastructure:

- Horizon Air Link (boot appliance).
- *smartnode*-sm1 (Horizon Cloud Node management appliance). The actual name of this appliance is automatically generated by the Horizon Air Link during the configuration process.

Management services, App Volumes, the Cloud Connector, and the Instant Clone engine are installed in the single management virtual appliance.

As appropriate for your organization's needs, you can also use Unified Access Gateway appliances to enable access to desktops by your end users who are external to your corporate network.

End users can use the following devices or methods to access desktops provided by a Horizon Cloud with On-Premises Infrastructure environment.

- Windows, OS X, Chrome, Linux, iOS, or Android Horizon Clients.
- Horizon Thin Clients
- HTML Access using a supported browser.

Suggested Workflow

You must deploy the Horizon Cloud with On-Premises Infrastructure environment on a hyper-converged infrastructure before you begin setting up virtual desktops in Horizon Cloud and making them available to your end users.

1. Install and configure the Horizon Air Link appliance on a hyper-converged infrastructure, as described in the *Installation and Configuration* information.
2. Pair the Horizon Air Link appliance with Horizon Cloud and perform basic configuration, which creates your Horizon Cloud Node, as described in the *Installation and Configuration* information.
3. Install and configure User Environment Manager to achieve persistence of user data, settings, and profile in the end users' virtual desktops, as described in the *Installation and Configuration* information and in the VMware App Volumes with Horizon Cloud Application Delivery Best Practices and Operations Procedures document at vmware.com.
4. Perform a domain join and domain bind to join the Horizon Cloud Node to your Active Directory domain, as described in "Register Your First Active Directory Domain with Your Horizon Cloud Node," on page 12.
5. Upload SSL certificates. See "Upload Certificates," on page 23 for details.
6. Create a master desktop image as described in Chapter 3, "Creating a Desktop Image," on page 25.
7. Create AppStacks as described in "Creating Applications for Use in a Horizon Cloud with On-Premises Infrastructure Environment," on page 44.
8. Convert the master to a desktop image in Horizon Cloud and create assignments using that image. See Chapter 4, "Creating Desktop Assignments," on page 35.
9. Add the AppStacks to the inventory and create assignments using them as described in Chapter 5, "Creating Assignments for Applications Using AppStacks," on page 43.
10. Configure persistence, as described in VMware App Volumes with Horizon Cloud Application Delivery Best Practices and Operations Procedures.

After the setup is complete, end users can launch desktops and their applications within those desktops.

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 with On-Premises Infrastructure 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 log in to the Administration Console after joining your Horizon Cloud Node with an Active Directory domain. You must then make a selection about the CEIP. You can change your selection to join or leave the CEIP at any time after that initial selection.

Procedure

1 Log in to the Administration Console.

2 Click  **> 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**.

Getting Started Using Your Horizon Cloud with On-Premises Infrastructure Environment

1

To perform administrative tasks in the environment, you use the cloud-based Administration Console. This user interface provides an integrated view and centralized access to manage virtual desktops and applications for delivery to your end users.

The Administration Console works in an industry-standard Web browser. For the list of supported Web browser types and versions, see the *Release Notes*.

Before you can perform administrative tasks, you must take your Horizon Cloud Node through the steps of registering at least one Active Directory domain, joining the domain to the node, and granting the super administrator role to one of your Active Directory groups. For details, see "Register Your First Active Directory Domain with Your Horizon Cloud Node," on page 12.

After completing those steps, a best practice is to follow the Getting Started wizard and perform the recommended actions.

You can also register and join additional Active Directory domains to enable assignment of virtual desktops from this Horizon Cloud Node to users in those domains, as well as configure auxiliary domain bind accounts to prevent locking your administrator users out of the Administration Console if the primary bind account becomes inaccessible.

This chapter includes the following topics:

Register Your First Active Directory Domain with Your Horizon Cloud Node

After you enter settings in the Horizon Cloud Node Setup user interface and run that process until you see the congratulations message, you connect to Horizon Cloud at cloud.horizon.vmware.com to register an Active Directory domain, perform the domain join and bind, and assign the super administrator role to at least one of the groups in that domain.

Note You must finish the entire Active Directory registration process for the first domain you are registering before you can perform other activities in the Administration Console. All services are locked until you finish these tasks.

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

Prerequisites

Ensure that the Active Directory infrastructure is synchronized to an accurate time source to prevent the domain join from failing. Such a failure requires you to contact VMware Support for assistance.

Verify that your Horizon Cloud Node is successfully deployed, to the point where the Setup congratulations message is available. See the *Installation and Configuration* information for details about the setup process.

For the required domain-bind account, verify you have the information for the Active Directory user account that adheres to the following guidelines:

- Is an Active Directory domain admin account.
- Has an account password that cannot expire, change, or be locked out.

Important You must use this account configuration because the system uses this account as a service account to query Active Directory.

For the required domain-join account, verify you have the information for the Active Directory user account that has domain-join permissions because the system uses this account to perform Sysprep operations on desktops and join the desktops to the domain. You can use the same account as the domain-bind account or a different one.

Procedure

1 Open a browser to Horizon Cloud at https://cloud.horizon.vmware.com.

2 Log in using your My VMware credentials.

The Administration Console opens and displays the Getting Started wizard.

3 In the Getting Started wizard, expand **General Setup** section if it is not already expanded.

4 Under Active Directory, click **Configure**.

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

Important Use an Active Directory account that adheres to the guidelines for the domain-bind account described in the prerequisites.

Option	Description
NETBIOS Name	Active Directory domain name
DNS Domain Name	Fully qualified Active Directory domain name
Protocol	Automatically displays LDAP.

Option	Description
Bind Username	User account in the domain to use as the LDAP bind account
Bind Password	The password associated with the name in the **Bind Username** text box.

You can optionally provide values for advanced properties.

Option	Description
Port	The default is **LDAP -> 389**. You do not need to modify this text box unless you are using a non-standard port.
Domain Controller IP	(Optional) If you want Active Directory traffic to use a specific domain controller, type a single preferred domain controller IP address. If this text box is left blank, the system uses any domain controller available for this Active Directory domain.
Context	LDAP naming context. This text box is autopopulated based on the information provided in the **DNS Domain Name** text box.

6 Click **Domain Bind**.

At this point, if the domain bind process succeeds, the Domain Join dialog box appears and you can continue to the next step.

If the domain bind process fails, you must restart the registration process by:

a Reloading the https://cloud.horizon.vmware.com URL in a new browser tab or page.

b At the login window, log in using your My VMware account credentials.

c At the Active Directory login window, log in using the LDAP bind account user name and password that you provided in the previous step.

d Continue with the next step.

7 In the Domain Join dialog box, provide the domain-join information.

Note Use an Active Directory account that adheres to the guidelines for the domain-join account described in the prerequisites. You can use the same account as the bind account used in Step 5 or a different one.

Option	Description
Join Username	User account in the Active Directory that has permissions to join systems to that Active Directory domain.
Join Password	The password associated with the name in the **Join Username** text box.
Primary DNS Server IP	IP address of the primary DNS Server
Secondary DNS Server IP	(Optional) IP of a secondary DNS Server

8 Click **Save**.

At this point, if the domain join process succeeds, the Add Super Administrator dialog box appears and you can continue to the next step.

If the domain join process fails, you must restart the registration process by:

a Reloading the https://cloud.horizon.vmware.com URL in a new browser tab or page.

b At the login window, log in using your My VMware account credentials.

c At the Active Directory login window, log in using the LDAP bind account user name and password that you provided in the previous step.

d Continue with the next step.

9 In the Add Super Administrator dialog box, use the Active Directory search function to select the Active Directory administrator group you want performing management actions on your environment using the Administration Console.

This assignment ensures that at least one of your Active Directory domain's user accounts is granted the permissions to perform management actions in the Administration Console now that the Horizon Cloud Node is joined to the domain.

10 Click **Save**.

The following items are now in place:

- The Horizon Cloud Node is joined to the Active Directory domain.
- Management activities in the Administration Console are now available.
- Logging in to the Administration Console to perform management tasks now has two parts: first a My VMware login to Horizon Cloud and then an Active Directory login to the Horizon Cloud Node using an account from the group with the super administrator role.
- Users in the group to which you granted the super administrator role can access the Administration Console and perform management activities.
- User accounts in the joined Active Directory domain can be selected for assignments using the Administration Console, such as desktop assignments.

What to do next

From this point, you typically perform the following tasks:

- Add one or more auxiliary bind accounts to this Active Directory domain configuration. If the primary bind account you specified becomes inaccessible, the system uses the auxiliary bind account to connect to the Active Directory domain. Having an auxiliary bind account avoids locking out your administrator users from the Administration Console in situations where the primary bind account is inaccessible in the Active Directory domain. See "Add an Auxiliary Bind Account for an Active Directory Domain Registered to Your Horizon Cloud Node," on page 18.
- Continue with the Getting Started wizard's steps. See "Getting Started Wizard for Your Horizon Cloud Node Environment," on page 16.
- Navigate to other areas of the Administration Console to perform management tasks. See Chapter 9, "About Menu Selections in the Administration Console," on page 73.
- If you have additional Active Directory domains with users to whom you want to grant management access to the Administration Console or end users to whom you want to give assignments, you can register those Active Directory domains also. See "Register Additional Active Directory Domains with Your Horizon Cloud Node," on page 16.
- Assign the demo administrator role to those users in this domain to whom you want to grant read-only access to the Administration Console. See "Assign Roles to Users for Administration Console Access," on page 24.

Log in to the Administration Console Used with Horizon Cloud Nodes

The Administration Console is a Web interface provided by the cloud service. You use an industry standard browser to log in to the interface. Some details of the login steps vary depending on the configuration of your specific environment.

You first log in using the My VMware credentials. The windows that display after the My VMware login window vary depending on your environment.

Environment	Window Displayed After the My VMware Login Window	What to Do Next
One Horizon Cloud Node No Active Directory domain joined to the node	Getting Started wizard and the General Setup section	Perform the domain join procedure and assign the super administration role to a user, as described in "Register Your First Active Directory Domain with Your Horizon Cloud Node," on page 12.
One Horizon Cloud Node One Active Directory domain joined to the node	Active Directory login window displaying the name of the joined domain.	Log in using credentials for an account in the joined domain.
One Horizon Cloud Node Multiple Active Directory domains joined to the node	Active Directory login window with a domain selection list.	Select a listed domain and log in using credentials for an account in the selected domain.
Multiple Horizon Cloud Nodes	Node-selection window displaying icons representing the nodes.	Select the node you want to work with in this session. The system displays the appropriate subsequent window depending on the number of Active Directory domains joined to the selected node.

Prerequisites

Verify that you have the credentials of the My VMware associated with the environment.

When an Active Directory domain is already joined, verify that you have the credentials for an Active Directory account in that domain that has access permissions.

Procedure

1 Navigate to the cloud service at `https://cloud.horizon.vmware.com`.

2 Log in with your My VMware credentials.

If your configured environment has more than one Horizon Cloud Node, a node-selection box appears and you select the Horizon Cloud Node you want to work with during this session.

To see a summary describing the node's downloading, building, readiness, and connection status, hover over each icon.

3 Depending on the options presented to you in the next window, complete the log-in sequence appropriate for your configured environment.

If the Horizon Cloud Node has a joined Active Directory domain, the Active Directory login window appears and you must log in with Active Directory credentials.

The Administration Console for the selected Horizon Cloud Node appears.

What to do next

If applicable, register the Active Directory and finish the domain join. See "Register Your First Active Directory Domain with Your Horizon Cloud Node," on page 12. You must finish the entire Active Directory registration process before you can work with any other services.

Getting Started Wizard for Your Horizon Cloud Node Environment

You use the Getting Started wizard to perform the configuration steps that are needed before you can fully manage and use the environment, such as registering an Active Directory domain. The Getting Started wizard displays when you log in to the Administration Console the first time after configuring a Horizon Cloud Node.

After you have finished registering one Active Directory domain, then you can perform administration tasks using the Administration Console, as well as register additional Active Directory domains, as appropriate for your organization's needs.

The Getting Started wizard provides a high-level overview of the work that you have done, and what is still to do. You can access the wizard at any time by clicking the  icon in the top right corner of the page.

Note To ensure that you completed all tasks required to run and manage the environment, review the steps in "Suggested Workflow," on page 8. You cannot perform certain tasks from the Getting Started wizard, such as uploading certificates.

Table 1-1. Getting Started Wizard Selections

Option	Description
Infrastructure	Displays details for the Horizon Cloud Node that is associated with the console's logged-in session.
General Setup	Provides details and links for configuring an Active Directory domain, roles and permissions, and file share registration. See Chapter 2, "General Setup Section of the Getting Started Wizard," on page 21.
Desktop Assignment	Provides links to pages where you can convert an image to a desktop, and create a desktop assignment. See Chapter 4, "Creating Desktop Assignments," on page 35.
App Assignment	Provides links to where you can create application assignments. See Chapter 5, "Creating Assignments for Applications Using AppStacks," on page 43.

During ongoing administration, the wizard is a convenient launching point for navigating to the console areas to perform typical administrative tasks. When you have completed the required steps of registering at least one Active Directory domain and setting a Super Administrator user, displaying the wizard is optional. To toggle having the wizard appear every time you log in to the Administration Console, use the **Show at Startup** slider at the bottom of the wizard's main page.

Register Additional Active Directory Domains with Your Horizon Cloud Node

You can optionally register additional Active Directory domains with your Horizon Cloud Node to assign management roles or provide assignments to users in those domains.

Prerequisites

Ensure that the Active Directory infrastructure is synchronized to an accurate time source to prevent the domain join from failing. Such a failure requires you to contact VMware Support for assistance.

For the required domain-bind account, verify you have the information for the Active Directory user account that adheres to the following guidelines:

- Is an Active Directory domain admin account.

- Has an account password that cannot expire, change, or be locked out.

Important You must use this account configuration because the system uses this account as a service account to query Active Directory.

For the required domain-join account, verify you have the information for the Active Directory user account that has domain-join permissions because the system uses this account to perform Sysprep operations on desktops and join the desktops to the domain. You can use the same account as the domain-bind account or a different one.

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.

Important Use an Active Directory account that adheres to the guidelines for the domain-bind account described in the prerequisites.

Option	Description
NETBIOS Name	Active Directory domain name
DNS Domain Name	Fully qualified Active Directory domain name
Protocol	Automatically displays `LDAP`.
Bind Username	User account in the domain to use as the LDAP bind account
Bind Password	The password associated with the name in the **Bind Username** text box.

You can optionally provide values for advanced properties.

Option	Description
Port	The default is **LDAP -> 389**. You do not need to modify this text box unless you are using a non-standard port.
Domain Controller IP	(Optional) If you want Active Directory traffic to use a specific domain controller, type a single preferred domain controller IP address. If this text box is left blank, the system uses any domain controller available for this Active Directory domain.
Context	LDAP naming context. This text box is autopopulated based on the information provided in the **DNS Domain Name** text box.

4 Click **Domain Bind**.

The Domain Join dialog box appears.

5 In the Domain Join dialog box, provide the domain-join information.

Note Use an Active Directory account that adheres to the guidelines for the domain-join account described in the prerequisites. You can use the same account as the bind account used in Step 3 or a different one.

Option	Description
Join Username	User account in the Active Directory that has permissions to join systems to that Active Directory domain.
Join Password	The password associated with the name in the **Join Username** text box.
Primary DNS Server IP	IP address of the primary DNS Server

Option	Description
Secondary DNS Server IP	(Optional) IP of a secondary DNS Server
Default OU	Active Directory organization unit to have the desktop image resources, such as `OU=NestedOrgName, OU=RootOrgName,DC=DomainComponent`. The system default is `CN=Computers`.

6 Click **Save**.

At this point, if the domain join process succeeds, the Add Administrator dialog box appears and you can continue to the next step.

7 In the Add Administrator dialog box, use the Active Directory search function to add a group from this Active Directory that you want performing management actions on your environment using the Administration Console.

8 Click **Save**.

The following items are now in place:

- The Horizon Cloud Node is joined to the Active Directory domain.
- After logging in to Horizon Cloud using your My VMware credentials, in the Active Directory login window, users with the super administrator role can select the domain that corresponds to their Active Directory account.
- Users in the group to which you granted the super administrator role can access the Administration Console and perform management activities.
- User accounts in the joined Active Directory domain can be selected for assignments using the Administration Console, such as desktop assignments.

What to do next

From this point, you typically perform the following tasks:

- Add one or more auxiliary bind accounts to this Active Directory domain configuration. If the primary bind account you specified becomes inaccessible, the system uses the auxiliary bind account to connect to the Active Directory. Having an auxiliary bind account avoids locking out your administrator users from the Administration Console in situations where the primary bind account is inaccessible in the Active Directory domain. "Add an Auxiliary Bind Account for an Active Directory Domain Registered to Your Horizon Cloud Node," on page 18.
- Assign the demo administrator role to those users in this domain to whom you want to grant read-only access to the Administration Console. See "Assign Roles to Users for Administration Console Access," on page 24.

Add an Auxiliary Bind Account for an Active Directory Domain Registered to Your Horizon Cloud Node

You can optionally configure an auxiliary bind account for the Active Directory domains that are registered with your Horizon Cloud Nodes. Configuring an auxiliary bind account avoids locking out your administrator users from the Administration Console in situations where the primary bind account is inaccessible in the Active Directory domain. If the primary bind account configured for the domain becomes inaccessible, the system uses this auxiliary bind account to connect to the Active Directory domain.

Prerequisites

Verify that the Active Directory domain is registered to the Horizon Cloud Node by navigating to **Settings > Active Directory** and seeing if the domain is listed on that page.

Verify that you have the user name and password information for the following accounts that are already configured in the Administration Console for the domain, because the user interface requires you confirm the existing passwords when performing this task:

- Password for the already configured bind account
- Password for the domain join account already configured in the user interface

Verify that you have the user name and password information for the bind account you are adding. Adhere to the following guidelines:

- Is an Active Directory domain admin account.
- Has an account password that cannot expire, change, or be locked out.

Important You must use this account configuration because the system uses this account as a service account to query Active Directory.

Procedure

1 In the Administration Console, click **Settings > Active Directory**.

2 Click the Active Directory domain for which you want to add the auxiliary bind account.

3 Click **Edit** next to the displayed domain bind settings.

4 In the Edit Active Directory dialog box, entering the password for the primary bind account.

Entering the password here makes the **Domain Bind** button available to click to save the changes.

5 Expand the advanced properties and click **Add Auxiliary Bind Account**.

A section for the auxiliary account information is added to the dialog box.

6 Type the account credentials.

Important Use an Active Directory account that adheres to the guidelines for the domain-join account described in the prerequisites.

7 Click **Domain Bind**.

8 In any subsequent windows that appear, confirm the existing settings by clicking **Save** in each window.

If the Domain Join window appears, type the password of the domain-join account before clicking **Save**.

The auxiliary bind account is available for the system to use if the primary bind account becomes inaccessible.

You can add multiple auxiliary bind accounts by repeating the steps. To change an auxiliary bind account's password or to remove it, use the corresponding links displayed in the Edit Active Directory window's advanced properties area.

General Setup Section of the Getting Started Wizard

2

In the first-time configuration for a Horizon Cloud Node, you use the choices in the General Setup section to configure the initial Active Directory domain settings, assign roles and permissions to Administration Console users, and configure one or more file shares to use for master image OVAs and the AppStacks that are generated by the AppCapture tool. After the first-time configuration, you can use the choices in the General Setup section to edit the initially configured Active Directory domain, refine the assigned roles, or navigate to the Locations page to work with the file shares.

Selection	Description
Active Directory	Register the initial Active Directory domain and add domain bind and domain join information. Domain registration of at least one Active Directory domain is required in order to give roles and permissions to Administration Console users or assign services to users. You must register an Active Directory domain and complete the domain join before you can perform other operations with the associated Horizon Cloud Node or register additional Active Directory domains. For information about tasks related to Active Directory and your Horizon Cloud Node, see: ■ "Register Your First Active Directory Domain with Your Horizon Cloud Node," on page 12 ■ "Register Additional Active Directory Domains with Your Horizon Cloud Node," on page 16 ■ "Add an Auxiliary Bind Account for an Active Directory Domain Registered to Your Horizon Cloud Node," on page 18
Roles & Permissions	Assign roles to users who will be managing the environment. A role grants its associated permissions to the users given that role. See "Assign Roles to Users for Administration Console Access," on page 24.
FileShare Location	Register one or more CIFS shares where you will copy the master image OVAs and the AppStacks that are generated by the AppCapture tool.

This chapter includes the following topics:

About File Shares

You register file shares with the Horizon Cloud Node to bring the AppStacks and the OVA files of the master virtual machines (VMs) into your Horizon Cloud with On-Premises Infrastructure environment. When the AppStacks and master VM OVAs are in the environment, you can begin using them for assignments to your end users.

File shares can be in the same domain as the Active Directory domain that is registered to the Horizon Cloud Node. They can also be part of a CIFS share. Horizon Cloud with On-Premises Infrastructure must have read permissions on your file shares.

When you register the file share with the Horizon Cloud Node, any master VM OVAs and AppStacks that are already present on the file share are automatically brought into your Horizon Cloud Node system. When you save new master VM OVAs to the registered file share, they are brought into your system when the system next polls the file share. When you save new AppStacks to the registered file share, they are not automatically brought into the system. To bring in new AppStacks, log in to the Administration Console and use the **Import** button on the file share

The system uses the master VM OVAs to generate the desktop images for end-user virtual desktops. Each OVA is an exported master VM file that you use when creating desktop assignments in the Administration Console. See "Export the Master Virtual Machine as an OVA File and Copy to Your File Share," on page 34.

You create AppStacks using AppCapture. See "Using AppCapture," on page 45. AppStacks that are already present in the file share are imported when you register the file share with the Horizon Cloud Node. To import AppStacks that you store on the registered file share, see "Import AppStacks," on page 56.

Register a File Share

Before you can bring master virtual machine (VM) OVA s and AppStacks into your Horizon Cloud with On-Premises Infrastructure environment, you must register a file share with your Horizon Cloud Node.

Procedure

1 Select **Settings > Locations** and click **File Share**.

2 Click **New**.

3 Provide the required information in the New File Share dialog box.

Option	Description
Name	Name of the file share.
Domain	Select the Active Directory domain that is registered to your Horizon Cloud Node and to the network file share.
Username	Admin user for the file share.
Password	Admin password for the file share.
Type	Type of file share.
Source Path	Path to the network file share, such as `\\share IP\sharename`.
Destination Pod	Virtual environment into which the master VM OVAs and AppStacks on this network file share are to be copied. The default destination is the virtual environment that matches your Horizon Cloud Node. To see the names of the available virtual environments, click in this box.

4 Click **Save**.

The location of this network file share is registered with your Horizon Cloud Node. Any master VM OVAs and AppStacks that are currently stored on the network file share are automatically brought into your Horizon Cloud Node system.

When you store additional AppStacks or new versions of the existing ones on the file share, use the **Import** button on the File Shares page to bring them into the system.

Upload Certificates

Upload SSL certificates to ensure that end users have a trusted connection to their environment.

Note During this procedure, the environment is temporarily unavailable and you cannot perform administrator operations. Upload the certificates after confirming that no users are on the system and no tasks, such as importing AppStacks, publishing images, provisioning desktops, assigning desktops, and so on, are running.

You must upload the `CA.crt` and `SSL.crt` files, and the `.key` private key.

The CA certificate and the SSL certificate must be in PEM format, which is a BASE64-encoded DER representation of an X.509 certificate. They both have a `.crt` extension, and look like this:

```
-----BEGIN CERTIFICATE-----
        MIIFejCCA2KgAwIBAgIDAIi/MA0GCSqG
        ..............
```

The private key must not have a password or passphrase associated with it. The `.key` file looks like this:

```
-----BEGIN RSA PRIVATE KEY -----
        MIIEpQIBAAKCAQEAoJmURboiFut+R34CNFibb9fjtI+cpDarUzqe8oGKFzEE/jmj

        ......................
```

Procedure

1 Select **Settings > General Settings**.

2 Click **Upload Certificate**.

3 For each of the certificate files listed in the Upload Certificate dialog box, click **Select** and navigate to the appropriate file.

4 When all of the certificate files are selected, click **Save**.

  The console will be unresponsive for 5 to10 minutes for all administrators while the certificates are applied.

5 When the system is responsive again, refresh the browser page and use your credentials to reauthenticate.

6 Verify that the certificates are valid on the General Settings page.

Assign Roles to Users for Administration Console Access

Use the Administration Console's role-based access control to determine who has access to manage your Horizon Cloud with On-Premises Infrastructure environment. The system provides two predefined roles that you can assign to your Active Directory groups.

Roles and their associated rights determine which management actions a user can perform using the Administration Console. The system provides two predefined roles. You must assign a role to your organization's appropriate Active Directory groups before the users in that group can log in to the Administration Console and access management actions.

Two predefined roles are provided by default: a super administrator role and a demo administrator role. The predefined roles cannot be modified.

Table 2-1.

Role	Description
Super Administrator	A mandatory role that you must assign to at least one group in your Active Directory domain and optionally to others. This role grants all the permissions to perform management actions in the Administration Console.
Demo Administrator	A read-only role that you can optionally assign to one or more groups. Demo administrators can view the settings and select options to see additional choices in the console, but the selections do not change the configuration settings.

NOTE To enable access to the Administration Console for users connecting from outside your corporate network, configure Unified Access Gateway. See the deploying and configuration information for Unified Access Gateway, available at the Unified Access Gateway product documentation page.

Procedure

- In the Administration Console, assign a role to Active Directory groups using one of the following methods.

Option	Description
From the Roles & Permissions section of the Getting Started wizard	a Click **Edit**. b Select one of the predefined roles. c Use the search box to search for and select an Active Directory group. d Click **Save**.
By navigating to Settings > Roles & Permissions	a Select one of the predefined roles and click **Edit**. b Use the search box to search for and select an Active Directory group. The group is added to the set of selected groups. c Click **Save**.

To remove the role from a group, click the **X** displayed on that group in the Selected User Group section.

Creating a Desktop Image 3

Before you can start assigning virtual desktops to your end users, you must create a desktop image that the system can use to spin out the virtual desktops. Creating a desktop image is a multi-step process.

1 First build a master virtual machine (VM), which includes several tasks to produce a master virtual machine that conforms to the Horizon Cloud environment's requirements.

2 Then copy this configured master VM to the file system that is joined to your Horizon Cloud Node and import it into the environment using the **Import** button on the Locations - File Shares page.

3 Use the New Image workflow in the Administration Console to convert the imported master virtual machine to a desktop image.

When the image on the Inventory - Images page displays the **Published** status, indicating it is ready for use, the system can use it in desktop assignments. At that point, you can assign the desktop image to end users. See "Create a Dedicated or Floating Desktop Assignment," on page 39.

This chapter includes the following topics:

Prepare for Building the Master Virtual Machine

You must obtain several items before you can build a master virtual machine (VM) that conforms to the Horizon Cloud environment's requirements.

Horizon Cloud with On-Premises Infrastructure supports using Microsoft Windows 7 and Microsoft Windows 10 (x86 and x64) as the guest operating system.

Important Take a snapshot after each main step so that you can revert to a known state if a problem occurs.

Procedure

1 Create a VM that has the Windows guest operating system that you want for your virtual desktops.

Use vSphere Web Client and vCenter Server, VMware Fusion® Pro, or VMware Workstation Pro™ to create a virtual machine and install the Windows guest operating system on it.

Build the master VM with a single virtual disk. Use hardware version 11 for vSphere 6.x environments.

Important

- When creating a master VM that you intend to use in the New Image workflow, a best practice is to use a single socket, single core master VM. If you have a master VM with multiple sockets and cores and you select it in the New Image workflow along with selecting the **Standard Desktop Model**, which specifies a single socket and core, the system automatically reconfigures the master VM to reduce the number of sockets and cores to one. This reduction might introduce instability on running virtual machines.
- When allocating RAM for the master VM, avoid choosing an overly conservative setting and take into account that insufficient RAM allocations can cause excessive Windows paging. Excessive Windows paging can generate I/O that causes significant performance degradations and increases storage I/O load. Configure video RAM in the master VM by editing the VM's hardware settings when it is powered off.
- Avoid joining the master VM to a domain. If the master VM is joined to a domain, unexpected results can occur when the system's VMware Instant Clone technology uses the domain-joined master VM to create the end users' virtual desktops.

---

2 Using the Administration Console, download the DaaS SSL bootstrap.

This file is used in the bootstrap process that allows the VM's guest operating system and the Horizon Cloud Node to pair with each other securely.

a Click **Inventory > Images**.

b On the Images page, select **... > Download Bootstrap**.

c In the download window, enter and re-enter a password of 8-20 ASCII characters containing at least one each of the following: lowercase letter, uppercase letter, number, and symbol (!@#$%^&*).

Do not use non-ASCII characters in the password. Make a note of this password for future use.

d Click **OK** to save the bootstrap file in a safe location for later use.

3 Find the IP address of the Horizon Cloud Node by navigating to **Settings > Infrastructure** in the Administration Console.

The Horizon Cloud Node IP address that is assigned from the desktop network is used in configuring the DaaS agent that is installed and configured in the master VM.

What to do next

Configure the master VM by following the steps in "Configure the Master Virtual Machine," on page 26.

Configure the Master Virtual Machine

You must perform several additional tasks to complete configuring the master virtual machine (VM) so that it can be used in the Horizon Cloud environment's New Image workflow.

You perform some of these steps in the VM's Windows guest operating system and others in the VMware software product in which you can configure the VM settings, such as the vSphere Web Client, Fusion Pro, or Workstation Pro.

For more information about the KMS Client Setup Keys, see https://technet.microsoft.com/en-us/jj612867.aspx.

Important Avoid joining the master VM to a domain. If the master VM is joined to a domain, unexpected results can occur when the system's VMware Instant Clone technology uses the domain-joined master VM to create the end users' virtual desktops.

Prerequisites

Complete all the steps outlined in "Prepare for Building the Master Virtual Machine," on page 25 and verify you have access to perform these steps on the VM you created.

Procedure

1 In the master VM's Windows guest operating system, enable the administrator account.

   a Open an elevated command prompt.

   b Enter `net user administrator /active:yes`.

   c Select **Control Panel > User Accounts** and set the administrator password.

2 Install VMware Tools in the VM.

   a Access the VM in the VMware product you used to create it, such as vCenter Server, Fusion Pro, or Workstation Pro.

   b Select the VM and use the menu options to select **Install/Upgrade VMware Tools**.

   c Click **OK**.

   d In the VM's Windows guest operating system, open an elevated command prompt.

   e Change directory to the CDROM drive.

   f When the VMware Tools installation finishes, restart the virtual machine for the changes to take effect.

3 In the Windows guest operating system's Control Panel, configure the network settings.

Setting	Values
Network	Name of network
DNS Servers	IP addresses of your DNS servers
IPv6	Disable (deselect check box)

4 In the virtual machine settings, set the adapter type to VMXNET 3 for the VM.

5 If your guest operating system is Microsoft Windows 7 SP1, install the network adapter hotfix for VMXNET 3 from https://support.microsoft.com/en-us/kb/2550978.

6 In the Windows guest operating system, install the required Windows updates as appropriate for your organization's needs.

7 Set up KMS for the Windows guest operating system.

Important Do not activate Windows on this master VM. The VMware Horizon Instant Clone Agent activates Windows for the clones during the agent's customization process.

a In the Windows guest operating system, open an elevated command prompt and enter **`slmgr /ipk`** ***`25-digit_license_key`*** to set up the Client Setup Key.

b Enter **`slmgr /skms`** ***`kms_server_IP_or_host_name:port`*** to specify your KMS server.

Note Do not activate Windows in the VM.

c Enter **`slmgr /dlv`** to verify setup and KMS server details.

What to do next

Perform the steps in "Optimize Guest OS Performance in the Master Virtual Machine," on page 28 and "Optimize Windows for Instant Clone Virtual Machines," on page 29, then install and configure the agents.

Optimize Guest OS Performance in the Master Virtual Machine

To improve the deployment performance of the virtual desktops that are generated from your master VM, take these steps to optimize performance of the VM's guest operating system.

Perform the steps in the VM's Windows guest operating system

Procedure

1 Disable, delete, remove, or turn off these items to optimize performance of the guest operating system.

Option	Action
Unused ports, such as COM1, COM2, and LPT	Disable.
Unnecessary services	Disable.
Indexing Service component	Disable. Indexing improves searches by cataloging files. Do not disable this feature for users who search often.
System Restore points	Remove or minimize.
Uninstall folders on `C:\Windows`, such as `$NtUninstallKB893756$`	Delete.
All event logs	Delete.
Setting that tracks the last time a file was accessed	Run the `fsutil` command to disable this setting. For example: `fsutil behavior set disablelastaccess 1`.
Set Disk Timeout on Windows Guest OS	Run the `regedit.exe` command to start the Registry Editor and change the TimeOutValue REG_DWORD in `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\Disk` to `0x000000be(190)`. After you make this change, Windows waits at least 190 seconds for delayed disk operations to complete before generating errors.
Disk Cleanup	Run to remove temporary and system files, empty Recycle Bin.
Disk Defragmenter	Run to rearrange fragmented data.
System protection on the C drive	Turn off.
Automatic computer maintenance	Turn off.
Tablet PC Components	Uninstall, unless you need this feature.

2 Adjust display properties.

   a Choose a basic theme.

   b Set the background to a solid color.

   c Set the screen saver to None.

   d Verify that hardware acceleration is enabled.

3 Select a high-performance power option and do not specify a sleep timer.

4 Set the sound scheme to **No Sounds**.

5 Set visual effects to **Adjust** for best performance.

6 Open Windows Media Player and use the default settings.

7 Turn off the Windows Customer Experience Improvement Program and disable related tasks from the Scheduler.

   These steps apply to Windows 7. The steps might vary for different Windows operating systems.

   a In the Windows 7 guest operating system control panel, select **Action Center > Change Action Center settings**.

   b Click **Customer Experience Improvement Program settings**, select **No, I don't want to participate in this program**, and click **Save changes**.

   c In the Task Scheduler (Local) pane of the Task Scheduler dialog box, select **Task Scheduler > Library > Microsoft**, expand the **Windows** nodes, and open the `Applications Experience` folder.

   d Disable the AIT Agent, ProgramDataUpdater, and if available, Microsoft Compatibility Appraiser tasks.

   e Open the `Autochk` folder and disable the Proxy task.

8 Shut down the guest operating system, power off the virtual machine, and power it back on.

Optimize Windows for Instant Clone Virtual Machines

Your Horizon Cloud with On-Premises Infrastructure system uses the VMware Instant Clone technology to rapidly clone and deploy virtual desktops from the desktop image built from your master VM. To reduce the growth of disk use by the instant clone VMs in the environment, you can disable certain services and tasks in your Windows 7 and Windows 10 guest operating systems.

The VMware Instant Clone technology uses the vSphere vmFork capability to quiesce a running base desktop image (the parent VM) and hot-clone it to create a pool of up to 1,000 instant clones. Instant clones share the virtual disks and memory of that base desktop at the time of creation. Each instant clone acts like an independent desktop, with a unique host name and IP address, but it requires less storage, reducing the capacity requirement by 50 to 90 percent. The overall memory requirement is also reduced.

The system can also customize the guest operating system of these instant clones during their initial booting process, to ensure that all instant clones join an Active Directory domain. Instant clones are always created in a power-on state and ready for users to log in.

After a user logs in and starts to use a virtual desktop, the capacity requirement grows. When the user logs out, the instant clone is refreshed and shrinks back to its original size.

By disabling certain Windows 7 and Windows 10 service and tasks, you can reduce the growth in disk use of instant clones that occurs while users are logged in. For more information about disabling these services, see Setting Up Desktop and Application Pools in View for VMware Horizon 7.

To optimize performance, disable these items in the Windows guest operating systems of your master virtual machines.

- Scheduled disk defragmentation
- Windows Update Service
- Diagnostic Policy Service
- Prefetch and Superfetch features
- Windows Registry backup
- System Restore
- Windows Defender
- Microsoft Feeds Synchronization

Install and Configure VMware Agents

In the master virtual machine's Windows operating system, install and configure the respective VMware agents in a specific order before you configure the DaaS Agent.

Prerequisites

- Verify that the master virtual machine is created and configured. See "Configure the Master Virtual Machine," on page 26.
- Verify that you have the agent installation files. You can download the files from http://www.vmware.com.

Procedure

1 Install the Horizon Agent.

   a Start the installer with the options appropriate for the environment in which you are building your master VM.

Option	Description
If building the master VM in a vCenter Server environment	Run the installer with `viewagent-installer.exe`.
If building the master VM in non-vCenter Server environments	Run the installer with `viewagent-installer.exe /vVDM_SKIP_BROKER_REGISTRATION=1`.

   b Deselect the **VMware Horizon View Composer Agent** option.

   c Select the **VMware Horizon Instant Clone Agent** option

   d Deselect the **VMware vRealize Operations Desktop Agent** option.

   e Reboot when prompted.

2 Install the DaaS Agent.

3 Run the App Volumes Unified Agent Installer and select the **Horizon Air Hybrid-Mode** check box in the installation screens.

What to do next

Configure the DaaS Agent by following the steps in "Configure the DaaS Agent," on page 31.

For improved security regarding the use of the Horizon Agent, configure your Active Directory server domain policy GPO (Group Policy Object) to disable weak ciphers in SSL and TLS protocols. For information about disabling weak ciphers when communicating using the SSL/TLS protocol, see the appropriate Horizon Agent information in the VMware Horizon 7 documentation set, such as Disable Weak Ciphers in SSL/TLS.

Configure the DaaS Agent

You can configure the DaaS Agent by using DHCP or by editing the `Monitor.ini` file located in the DaaS Agent installation directory in the master virtual machine's Windows guest operating system.

Prerequisites

- Find the IP address of the Horizon Cloud Node by navigating to **Settings > Infrastructure** in the Administration Console. The Infrastructure page reports the IP address. For additional information, see "Determine the Horizon Cloud Node IP Address for Use by Desktops," on page 81.

  Note This IP address was formerly referred to as the tenant appliance IP address or tenant IP address. You might see the labels in the Administration Console reflecting that former name.

- Install the DaaS Agent by following the steps in "Install and Configure VMware Agents," on page 30.
- Download the DaaS SSL bootstrap. See "Prepare for Building the Master Virtual Machine," on page 25.
- In the master VM's Windows guest operating system, open a command prompt as administrator, navigate to the DaaS Agent installation directory, and navigate to the service directory in that installation directory, such as:

  ```
  C:\Program Files (x86)\VMware\VMware DaaS Agent\service
  ```

- Confirm that you can access the `Keytool.exe` file from the Windows guest operating system.

  You can ensure that the `Keytool.exe` file is accessible by copying it to the Windows guest OS or accessing it through a network file share.

- In the Windows guest operating system, run `Keytool.exe` using the DaaS SSL bootstrap file as an argument.

  ```
  Keytool.exe -f "absolute path for bootstrap file"
  ```

  When prompted, enter the encryption password that you set when you downloaded the DaaS SSL bootstrap file using the steps in "Prepare for Building the Master Virtual Machine," on page 25.

  The `Keytool` utility performs the bootstrap and moves the certificate to the cert folder.

Procedure

- Configure the DaaS Agent using whichever method best suits your needs. However, DHCP is the recommended configuration option.

Option	Description
Use DHCP	a On your DHCP server, select **Control Panel > Administrative Tools** to open the DHCP configuration client. b Right-click **Server Options** and select **Configure Options**. c Locate the DHCP scope for the desktop network subnet. d Right-click the scope and click **Scope Options** to configure the 074 option code for that scope only. Configuration is the same as for the entire DHCP server. If you defined limited addresses, you can confine the configuration of the options to a specific scope. Configuration is the same as for the entire DHCP server. e Scroll down to the 074 option for Internet Relay Chat (IRC) and select the check box. f Add the Horizon Cloud Node IP address that you obtained from the Infrastructure page.
Enter the `Monitor.ini` File	a In the Windows guest operating system, navigate to the directory that contains the `MonitorAgent.ini` file. ■ 64-bit: `C:\Program Files (x86)\VMware\Vmware DaaS Agent\service` ■ 32-bit: `C:\Program Files\VMware\Vmware DaaS Agent\service` b Open the `MonitorAgent.ini` file for editing. c In the `[element]` section, uncomment the `standby_address` and add the Horizon Cloud Node IP address that you obtained from the Infrastructure page. For example: `standby_address=10.31.5.20` d Set auto discover to 0. e Save and close the file.

Using VMware Horizon Smart Policies for Your Desktops

A Horizon Cloud with On-Premises Infrastructure 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 Horizon Cloud with On-Premises Infrastructure environment, see the document titled VMware App Volumes with Horizon Cloud Application Delivery Best Practices and Operations Procedures at vmware.com.

The User Environment Manager Management Console runs on Windows. You can install it on a Windows VM running on your Horizon Cloud Node or on a Windows VM or machine from which you want to manage the User Environment Manager environment.

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.

- Run the App Volumes Unified Agent Installer to install the required agents on the master VM, as described in "Install and Configure VMware Agents," on page 30. 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 with On-Premises Infrastructure 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 with On-Premises Infrastructure 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 `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 `ViewClient_Broker_GatewayLocation` property is set to `Internal` and `ViewClient_Broker_GatewayType` property is set to `AP`.

As stated in the *Installation* guide, using a Unified Access Gateway with your Horizon Cloud with On-Premises Infrastructure environment is a best practice. However, if you do not have a Unified Access Gateway, the broker sets the `ViewClient_Broker_GatewayLocation` property to `Internal` and the `ViewClient_Broker_GatewayType` property to `None`.

Export the Master Virtual Machine as an OVA File and Copy to Your File Share

After you configure the agents, you export the master virtual machine (VM) from where you were configuring it and copy it to the file share that is registered with your Horizon Cloud Node. You must export the master VM as an OVA file and copy that OVA file to the file share. The system picks up the OVA file and makes it available in the environment so that you can run the New Image workflow to create a desktop image.

Prerequisites

- Verify that a network file share is registered with your Horizon Cloud Node. See "Register a File Share," on page 22.
- Verify that you have a master VM that is configured and the required agents installed and configured according to the steps in "Configure the Master Virtual Machine," on page 26, "Install and Configure VMware Agents," on page 30, and "Configure the DaaS Agent," on page 31.
- Verify that you can export the master VM as an OVA file from the software you used to configure it, such as from vCenter Server, Workstation Pro, or Fusion Pro.

Procedure

1 Export the master VM as an OVA file, saving the file to a location from which you can copy it to the file share.

2 Copy the OVA file to the root directory of the file share.

NOTE Subfolders on the file share are not supported.

The system polls the file share at regular intervals. When the system detects the added OVA, the system automatically deploys it to your environment and powers it on. The time it takes to deploy the OVA and power it on depends on the speed of the network between the file share and your Horizon Cloud Node and the size of the OVA file.

What to do next

Verify the VM is available for use in the New Image workflow by navigating to **Inventory > Imported VMs** and seeing that the VM is listed on that page.

Run the New Image workflow and create a desktop assignment using this master VM. See "Convert a Desktop to an Image Using the New Image Workflow," on page 35.

Creating Desktop Assignments

4

Before your end users can work with virtual desktops provided by your Horizon Cloud with On-Premises Infrastructure environment, you have to use the Administration Console to create desktop assignments. Before you can create a desktop assignment, you must have a desktop image in the system that the system can assign, an image in the **Published** state. This image is used as the operating system on the virtual desktops.

The Administration Console provides the following navigation paths to create desktop assignments. You can start from the Getting Started wizard or perform the actions using the individual Images and Assign screens. First you create the image using the New Image workflow, and then you create a desktop assignment referencing that image.

Action	From the Getting Started wizard	From any location in the Administration Console
Create the image using the New Image workflow. See "Convert a Desktop to an Image Using the New Image Workflow," on page 35.	**Desktop Assignment > Create Image > New**	**Inventory > Images > New**
Create the desktop assignment. See "Create a Dedicated or Floating Desktop Assignment," on page 39.	**Desktop Assignment > Create New Desktop Assignment > New**	**Assign > New > Desktops**

This chapter includes the following topics:

Convert a Desktop to an Image Using the New Image Workflow

To turn a configured master virtual machine (VM) into an assignable desktop image, use the Image page's New Image workflow. A desktop image must display the Published status on the Images page before you can assign to end users for their virtual desktops.

Prerequisites

Verify that a master VM is available in your environment. See "Export the Master Virtual Machine as an OVA File and Copy to Your File Share," on page 34.

Verify that the Imported VMs page indicates that the master VM is powered on (green status).

Procedure

1 In the Administration Console, select **Inventory > Images** and click **New**.

2 Enter the required information.

Option	Description
Desktop	Start typing the first few letters of the master virtual machine name. All desktops that the system can convert to an image appear. Select the name when it appears. **Note** It can take approximately 10 minutes after the master VM is imported from the file share for the inventory to display. After you select a desktop name, the **Image Name** text box is auto-populated.
Image Name	You can edit the auto-populated image name in this text box.
Domain	Select the Active Directory domain that you want to use with this desktop image. The Active Directory domains that are registered to this Horizon Cloud Node appear in the list.
Company Name	Type an identifying name.
Timezone	Retain the default.

3 Click **Publish**.

The publishing process takes several minutes to complete. The page displays the **In Transition** status during this process. You can use the refresh icon to see the latest status.

If the process is successful, the image's status is **Published**. Also, the Imported VMs page no longer displays the master VM now that it has been converted to a desktop image.

If the publish operation fails, select **Monitor > Activity** and locate the failed job. Correct the problem, then retry the publish operation by selecting the check box next to the image, clicking **... > Convert to Desktop**. Then click **New**, enter the required information, and click **Publish** to publish the image.

Note Do not restore a master VM to a snapshot taken before the DaaS Agent bootstrapping process and then try to convert it to a desktop. If the agent has already been bootstrapped, reverting the virtual machine to a snapshot prevents the agent from communicating properly.

Actions You Can Perform on Images

You can perform several actions on the images listed on the Administration Console's Images page.

Procedure

1 Select **Inventory > Images**.

2 Select the check box next to the image on which you want to perform an action.

3 Perform an action on the image according to the selection method.

To rename or duplicate an image, click the appropriate button.

Button	Description
Rename	Enter a new image name and click **Save**.
Duplicate	Enter a new name and click **Save**.

To perform one of the other available actions, click **...** and select the drop-down option of your choice.

Drop-Down Option	Description
Delete	Permanently deletes the selected image.
Convert to Desktop	Converts the selected image to a desktop.
Assign Image	Assigns the updated image to the selected desktop assignment. Select the assignment from the list and click **OK**.
Download Bootstrap	Downloads an encrypted bootstrap file for you to deploy to your images. When you select this option, you are 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 (!@#$%^&*). Do not use non-ASCII characters in the password.
Refresh Password	If you refresh the password 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.

Update Image and Push Changes to Desktop Assignments

After you publish your initial image and create your desktop assignments, you can make changes to that image and push the changes to the existing desktop assignments that are using that image.

You can update the image in place in your Horizon Cloud Node's vCenter Server environment by making a copy of the image. You can also update the image offline (outside of the vCenter Server environment) and drop the new images to the file share associated with the node.

Important If you perform the update offline, make sure that the OVA file has a different internal name than the previous image that you are replacing. Images with duplicate names fail to deploy to the vCenter Server environment.

Procedure

1 Select **Inventory > Images** and select the check box next to your image.

2 Click **Duplicate**, name the new virtual machine and click **Save**.

3 Select **Monitor > Activity** to track the copy process, and verify that the status is successful.

It can take a few minutes for the desktop to be available for selection after the copy process finishes.

4 Select **Inventory > Images** and select **New**.

5 In the **Desktop** text box, start typing the name of your new master virtual machine and select it from the drop-down menu.

A warning message indicates that your virtual machine is currently powered off.

6 Select **Power On**, wait for the **IP Address** field to populate, then click the IP address to download an RDP file.

7 Click the RDP file, connect to your virtual machine, and make the required changes to your image.

8 Click **Publish**.

Wait until the publish operation finishes and the image is online before continuing.

9 Select **Inventory > Images** and select the check box next to your new image.

10 Select **...**, click **Assign Image**, select the assignments to update, and click **OK**.

The system deletes each virtual machine in the selected assignment and recreates it using the new image. If a user is logged into a desktop when you push the updates, the system does not update that desktop until the user logs off.

11 If no other assignments are using the original image and you want to delete it, select **...** and click **Delete**.

Types of Desktop Assignments

You can create different types of desktop assignments to fit your end-user environment needs.

You can create dedicated and floating desktops assignments in your Horizon Cloud with On-Premises Infrastructure environment.

Note A desktop can have multiple users assigned to it, but it can be used by only one user at a time.

- 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. For example, you need an assignment of one hundred desktops for a group of one hundred users. The primary use for dedicated desktop assignments is to ensure that the host name of the desktop virtual machine for each user remains the same between sessions. Certain software packages might require this use for licensing.
- In a floating desktop assignment, a user receives a different virtual machine with a different machine name with each login. With floating desktop assignments, you can create desktops that shifts of users can use and that should be sized based on the maximum number of concurrent users. For example, three hundred users can use an assignment of one hundred desktops if they work in shifts of one hundred users at a time. With floating desktop assignments, the user might see different host names for each desktop session.

Note Neither floating nor dedicated desktops provide persistence. Both types are reset after each user session. You can configure persistence for user-installed applications by creating writable volumes. See Chapter 6, "Working with Writable Volumes," on page 59.

Persistence of user data, settings, and profiles is handled by the VMware User Environment Manager® software components in your Horizon Cloud with On-Premises Infrastructure environment. For information on configuring persistence of those items, see these resources:

- The *VMware User Environment Manager Deployment Considerations* document at http://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/techpaper/vmware-user-environment-manager-deployment-considerations.pdf.
- The User Environment Manager documentation.

Where possible, use floating desktop assignments because they provide more flexible pool management capabilities than dedicated desktop assignments and they avoid dedicating virtual machine resources for each user.

Create a Dedicated or Floating Desktop Assignment

You can create desktop assignments using the Assignments page or from the Getting Started wizard.

Note

- When you use the Blast Extreme or PCoIP display protocols, the correct video RAM value is dependent on the number of displays configured for end users and on the display resolution. The typical recommendation for a four monitor setup is 128 MB. For lower screen resolutions or fewer monitors, configure lower video RAM to save base memory for additional desktops.
- When allocating RAM for the master VM, avoid choosing an overly conservative setting and take into account that insufficient RAM allocations can cause excessive Windows paging. Excessive Windows paging can generate I/O that causes significant performance degradations and increases storage I/O load. Configure video RAM in the master VM by editing the VM's hardware settings when it is powered off.
- If you require the desktop image to be registered against an OU in Active Directory other than CN=Computers, you can use the General Settings page to configure that required OU as a default. See the Image Defaults Configuration option.

For more information about desktop assignments, see "Types of Desktop Assignments," on page 38. For more information about Active Directory, see "Working with Nested Organizational Units," on page 41.

Prerequisites

Verify that you have at least one image listed on the Images page. You cannot create a desktop assignment without an image available in the system. See "Convert a Desktop to an Image Using the New Image Workflow," on page 35.

Procedure

1 Open the New Assignment window by using one of these methods.

   - In the Getting Started wizard, click **Desktop Assignment > Go** for the Create New Desktop Assignment option.

     If a desktop assignment has not been created yet, the button in the Getting Started wizard is **New** instead of **Go**.
   - From any location in the Administration Console, click **Assign > New**.

2 In the New Assignment dialog box, click **Get Started** in the Desktops selection.

3 Select the type of assignment to create, provide the required information to configure the desktop assignment, and click **Next** to advance to the next step in the wizard.

Note Windows 10 operating systems perform better with desktop models other than the Standard Desktop Model, because the other desktop models provide more memory. Even though you can use the Standard Desktop Model with Windows 10, as a best practice only do so for light workloads and basic applications.

Option	Description
Desktop Model	Select model from the drop-down list. After you select a desktop model, the **Image** text box is auto-populated.
Image	Select your image.
Assignment Name	Type a unique name for the new assignment.

Option	Description
Default Protocol	Select a default display protocol, Blast or PCoIP. 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 desktops from the Workspace™ ONE™ portal, either a Horizon Client or a browser for HTML Access. ■ Browser ■ Horizon Client
Capacity	Select the number of desktops required in the assignment.

Optionally configure the advanced properties.

Option	Description
VM Names	Name for all virtual machine names, or guest desktops in this assignment. When the guest desktops are deployed in the system, their names include the name specified here plus a number appended to it, such as win7-1, win7-2, and so on. This name must start with a letter and can contain only letters, dashes, and numbers. This value is prefilled based on the assignment name.
Computer OU	Active Directory (AD) Organizational Unit where the desktop VMs are to be 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.
Run Once Script	(Optional) Location of scripts that you want run after system preparation completes.
Session Timeout Interval	The timeout value for floating and static desktop session pools. The default is seven days (10,080 minutes). The maximum value is 99,999 minutes, approximately 69 days. **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 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.

4 (Optional) On the Active Directory Search page, start typing the name of a user or group from your Active Directory.

5 Select a user or group from the list.

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

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

The system begins the process of creating the virtual desktops. On the Assignments page, the Status column reflects the current progress.

Note If the Administration Console does not automatically load the Assignments page, you can return to it by clicking the **Assign** icon.

What to do next

To create additional desktop assignments, repeat Step 1 through Step 7.

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** text box. You cannot specify a nested OU in that text box. You must locate the nested OU information for your organization, then manually enter it in the **Computer OU** field.

Procedure

1 From your Active Directory machine, 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 Desktops Assignment page.

Only the `OU=` part of the string is required. The `DC=` part is optional.

Creating Assignments for Applications Using AppStacks

5

Before your end users can work with the AppStacks provided by your Horizon Cloud with On-Premises Infrastructure environment, you have to use the Administration Console to create assignments for them. Before you can create an assignment to an AppStack, the AppStack must be imported into the environment from the file share registered with your Horizon Cloud Node.

The Administration Console provides the following navigation paths to create these application assignments. You can start from the Getting Started wizard or perform the actions using the Assign screens.

Note You perform the AppCapture step outside of the Administration Console.

Action	From the Getting Started wizard	From any location in the Administration Console
Capture the application as an AppStack You run the App Volumes AppCapture utility to scan your available applications and create the AppStack files. Then you add those files to the file share. See "Creating Applications for Use in a Horizon Cloud with On-Premises Infrastructure Environment," on page 44.	Even though this step is listed in the Getting Started wizard's App Assignment section, you perform the steps outside of the Administration Console. The wizard displays this step as complete when the AppStacks are imported into the inventory. See "About the Inventory Icon," on page 76.	You perform the steps outside of the Administration Console.
Verify the AppStack is imported into the inventory. If not, import it using the Locations - File Share page. See "Import AppStacks," on page 56.	**App Assignment > App Inventory > Go**	**Inventory > Applications**
Create the application assignment. See "Create an Application Assignment," on page 57.	**App Assignment > Create New App Assignment > New**	**Assign > New > Applications**

In addition to AppStacks, the system uses its underlying App Volumes capabilities to support using ThinApp virtual applications. App Volumes delivers ThinApp instances as VMDKs. See the VMware technical white paper ThinApp Virtual Applications with CloudVolumes Shared VMDKs for details.

This chapter includes the following topics:

Creating Applications for Use in a Horizon Cloud with On-Premises Infrastructure Environment

You use AppCapture to create AppStacks for provisioning applications to user groups. Then you use User Environment Manager with folder redirection to provide persistence of end-user data, settings, and profiles.

Capturing Applications as AppStacks

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.

Using User Environment Manager for Persistence

A Horizon Cloud with On-Premises Infrastructure environment uses the VMware next-generation desktop and application delivery platform known as JMP (Just-in-Time Management Platform). JMP is a set of VMware technologies that deliver Just-in-Time desktops and applications. The JMP technologies applicable in a Horizon Cloud with On-Premises Infrastructure environment are:

- VMware Instant Clone Technology, providing fast desktop provisioning for your environment's virtual desktops
- App Volumes, providing real-time application delivery into those desktops
- User Environment Manager, providing contextual policy management

User Environment Manager provides various options for achieving the persistence of end-user data, settings, and profiles of virtual desktops. For a Horizon Cloud with On-Premises Infrastructure environment, the best practice is using User Environment Manager with folder redirection. A pre-defined configuration is available from VMware. For details about this pre-defined configuration along with the best practices for using App Volumes and User Environment Manager with your environment, see the document titled VMware App Volumes with Horizon Cloud Application Delivery Best Practices and Operations Procedures at vmware.com. This document also includes detailed information on the installation and setup of User Environment Manager for use with Horizon Cloud with On-Premises Infrastructure.

AppCapture System Requirements

Review these AppCapture minimum requirements for Windows platforms.

AppCapture System Requirements

To install and run AppCapture, you must 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.

Install AppCapture

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

Prerequisites

Ensure that you do not have the Horizon Cloud with On-Premises Infrastructure 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 Horizon Cloud with On-Premises Infrastructure 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 (Optional) Verify that `AppCapture.exe` is installed in `C:\Program Files\VMware\AppCapture` (64-bit machines) or `C:\Program Files\VMware\AppCapture` (32-bit machines).

What to do next

The UEM Application profiler is also installed with the AppCapture utility. You can personalize AppStacks using the UEM Application profiler.

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 either from a command line 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," on page 47 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.

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," on page 47.

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 process 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 the ThinApp feature is available in your environment, you can also capture ThinApp MSI packages. You can install these packages in the same way that you install other application MSI packages. See the latest VMware ThinApp documentation for information about how to create ThinApp MSI packages.

5 Finish creating the virtual disks.

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 the process.

After the reboot, you see new AppStacks containing applications.

c Verify that you have new VHD and VMDK files in `C:\ProgramData\VMware\AppCapture\appvhds`.

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 the file share connected with your environment.

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 5-1. `AppCapture.exe` Command-line Options

Task	Option
Display help for the `AppCapture.exe` command.	`/?`
Specify an author's name for the AppStack. If the name contains at least one space, put the name in parentheses. Example: **`AppCapture.exe /n /a (IT Admin)`**	`/a`
Specify a description for an AppStack. Example: **`This disk contains XYZ suite of applications.`**	`/d`
List the contents of the AppStack JSON, VHD, and VMDK files. If you are not using the default directory, specify the directory where the files are located. Example: **`AppCapture.exe /list filePath`**	`/list`
Generate a `.json` file by using a VMDK file as input. If you are not using the default path, specify the path containing the VMDK file. Example: **`AppCapture.exe /meta appStackPath`**.	`/meta`
Create an AppStack. Example: **`AppCapture.exe /n`**	`/n`
Specify an output directory for the AppStack files. The default directory is `C:\ProgramData\VMware\AppCapture\appvhds`. You can use this option with the `/s` option to create an AppStack from an existing AppStack. See "Update an AppStack from the Command Line," on page 50. Example: **`AppCapture.exe /s oldAppStackDir /o newAppStackDir`**	`/o`

Table 5-1. `AppCapture.exe` Command-line Options (Continued)

Task	Option
Specify a source directory for the AppStack files. The default directory is `C:\ProgramData\VMware\AppCapture\appvhds`. Do not use this option if you are installing a new application. You can use this option with the `/o` option to create an AppStack from an existing AppStack. See "Update an AppStack from the Command Line," on page 50. Example: **`AppCapture.exe /s oldAppStackDir /o newAppStackDir`** You can also use the `/s` option with `/n` to update an old AppStack with a new one. In this example, the existing *oldAppStack.vhd* AppStack is copied as a base AppStack and can be updated as *newAppstackName*: **`AppCapture.exe /n newAppstackName /s oldAppStack.vhd /o newAppStackDir`**	`/s`
Create a `.vhd` file from a `.vmdk` file. If you are not using the default path, specify the path containing the `.vhd` file. Example: **`AppCapture.exe /vhd appStackPath.vmdk`**	`/vhd`
Generate a VMDK file by using a VHD file as input. If you are not using the default path, specify the path containing the `.vhd` file. Example: **`AppCapture.exe /vmdk appStackPath.vhd`**.	`/vmdk`

Table 5-1. `AppCapture.exe` Command-line Options (Continued)

Task	Option
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. Example: **`AppCapture.exe /test Provisioned appStackPath.vhd`** Virtualize all application bundles in the AppStack. Example: **`AppCapture.exe /test Provisioned appStackPath.vhd *`** Virtualize application bundles that are identified by their corresponding GUIDs in the AppStack. Example: **`AppCapture.exe /test Provisioned appStackPath.vhd GUID1, GUID2.. GUIDn`**	`/test <Provisioned AppStackPath>.vhd [* | GUID]`
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. Example: **`AppCapture.exe /personalize C:\FinanceApps.vhd`** - Personalization settings are saved under `C:\ProgramData\VMware\AppCapture\appvhds\UEMConfigFiles\FinanceApps`. 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. Example: **`AppCapture.exe /personalize C:\FinanceApps.vhd /predef`** - Personalization settings along with predefined settings are saved under `C:\ProgramData\VMware\AppCapture\appvhds\UEMConfigFiles\FinanceApps` The `/flexconfigname` sub-option can be used with the `/personalize` command to store the personalization settings into a user-friendly configuration file name. Example: **`AppCapture.exe /personalize C:\FinanceApps.vhd /flexconfigname MSOffice2016`** - Personalization settings are saved under `C:\ProgramData\VMware\AppCapture\appvhds\UEMConfigFiles\MSOffice2016`	`/personalize <ProvisionedAppStackPath>.vhd [/predef | flexconfigname <flexconfigfilename> ]`

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.
- `/meta`. Creates a JSON file from the output 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," on page 47.

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.
- Disable User Account Control (UAC) notifications on the provisioning machine. See http://windows.microsoft.com/en-us/windows/turn-user-account-control-on-off#1TC=windows-7.
- Become familiar with the command options that apply to updating an AppStack. See "AppCapture Command-Line Options," on page 47).

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.

Task	Action
Add applications or update existing applications	Run the installers for the applications that you want to install or update on the AppStack.
(Optional) Remove applications	1 Navigate to **Control Panel > Programs and Features**. 2 Select the applications that you want to remove from the AppStack and complete the uninstall procedure.

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," on page 46.

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.
- Disable User Account Control (UAC). See http://windows.microsoft.com/en-us/windows/turn-user-account-control-on-off#1TC=windows-7
- Become familiar with the AppCapture cmdlets. See "PowerShell Options and Parameters," on page 52

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 5-2. `Start-AVAppCapture` Options

`Start-AVAppCapture` Parameter	Description
`-Author` *Author-name*	Specify an author who is associated with this AppStack.
CommonParameters	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: ■ Debug ■ ErrorAction ■ ErrorVariable ■ OutBuffer ■ OutVariable ■ PipelineVariable ■ Verbose ■ WarningAction ■ WarningVariable For more information about common parameters, see about_CommonParameters.
`-Description` *text*	Specify a description for an AppStack. If the description includes a space, enter the description inside parentheses, for example, **`-Description (HR Apps)`**.
`-Destination` *output-directory*	Specify an output directory for an AppStack. By default, AppStacks are placed in `C:\ProgramData\VMware\AppCapture\appvhds`.
`-Force`	Create an output directory if it does not exist. You specify the output directory with the `-Destination` parameter.
`-Name` *vhd-name*	Specify a name for the applications being captured. The output `.vhd` file is named by using the specified application name.
`-Novmdk`	Specify this option to prevent post-capture VMDK disk creation.
`-Path` *directory-path*	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.

You can perform several workflows with the AppCapture command.

Table 5-3. AppCapture PowerShell Workflows

Workflow	Description
`ConvertTo-AVVhdDisk`	Generate a `.vhd` file by using the `.vmdk` file as input.
`ConvertTo-AVVmdkDisk`	Generate a `.vmdk` file by using the `.vhd` file as input.
`Export-AVMetadata`	Generate a `.json` file by using a `.vhd` or `.vmdk` file as input.
`Merge-AVAppDisks`	Merge AppStack `.vhd` files into a new AppStack `.vhd`. "Merging AppStacks," on page 49 describes the command-line version, which is similar.
`Remove-AVApp`	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.

Table 5-3. AppCapture PowerShell Workflows (Continued)

Workflow	Description
`Reset-AVConfig`	Clear AppCapture configuration information from the machine
`Show-AVDiskDetails`	List the contents of the `.vhd` file, `.json` file, or `.vmdk` file.
`Start-AVAppCapture`	Start the procedure to capture applications.
`Start-AVAppUpdate`	Update an AppStack.
`Test-AVAppStack`	Attach or virtualize applications after provisioning the application.
`Start-AVAppPersonalization`	Attach the AppStack (`.vhd`) and personalize the specified application bundle using the UEM Application Profiler.

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.

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

- `ConverTo-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:

  `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`:

  `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 `C\temp`.

  `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:

  `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-AVAppUdate`. 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 5-4. AppCapture PowerShell Workflow Information and Examples

Command	Description
`get-help` *`WorkFlowName`*	View general information for a workflow.
`get-help` *`WorkFlowName`* `-detailed`	View detailed information for a workflow.
`get-help` *`WorkFlowName`* `-examples`	View an example of a workflow.
`get-help` *`WorkFlowName`* `-full`	View technical information for a workflow.

AppCapture Folders and Files

AppCapture creates several files and folders.

AppCapture creates various folders in `C:\ProgramData\VMware\AppCapture\appvhds`.

Table 5-5. AppCapture Folders

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

AppCapture creates these files in the `appvhds` directory unless you specify a different directory. See "AppCapture Command-Line Options," on page 47.

Table 5-6. AppCapture Files

File	Description
application`.vhd`	`.vhd` file that holds the application files that are part of the AppStack.
application`.vmdk`	VMDK-format Virtual Hard Disk file that Horizon Cloud with On-Premises Infrastructure natively uses.
application`.json`	The `.json` file with information about the applications that are captured in the AppStack.

Copy AppStacks to File Shares

After you have created your AppStacks, you must place them in file shares. Then you can assign the applications in the AppStacks to user groups.

Procedure

1 Open a File Explorer window for `\\`*`share IP`*`\sharename`

This is the file share where the AppStacks go. This file share is the file share that you configure using the Administration Console.

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 with On-Premises Infrastructure 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 AppStacks to file shares, you must synchronize the file shares by using Horizon Cloud with On-Premises Infrastructure. See "Import AppStacks," on page 56.

Import AppStacks

Any time you add applications to a file share, you must import the AppStacks from the external file share to the internal datastore.

Procedure

1 Navigate to **Settings > Locations**.

2 Click **File Share**.

3 Select the check box for the file share that has the AppStack to import.

You can import only one file share at a time.

4 Click **...** and select **Import**.

Delete an AppStack

You can use the Administration Console to delete AppStacks from the internal datastore.

Prerequisites

Confirm that the AppStack is not needed by end users before you delete it.

Note

- End users cannot use an AppStack after you delete it. The deletion might also impede user functionality.
- The system does not allow you to delete an AppStack that is in use.

Procedure

1 In the Administration Console, select **Settings > Storage Management**.

2 On the AppStacks page, select the check box next to the AppStacks you want to delete.

3 Click **Delete**.

A confirmation dialog box appears.

4 Click **Delete** again.

A message appears informing you that the deletion either failed or succeeded.

5 Navigate to the file share location and delete the AppStack.

If you do not delete the AppStack from the file share, the AppStack reappears on the AppStacks page after the next import takes place.

Create an Application Assignment

After you create a desktop assignment and import your App Stacks, you can create an application assignment.

Procedure

1 On the Getting Started page, expand the **App Assignment** section if necessary and click **Go** for the Create New App Assignment option.

2 On the Assignments page, click **New**.

3 In the New Assignment dialog box, click **Get Started** in the Applications section.

4 Provide the required information to configure the application assignment.

Option	Description
Assignment Name	Unique name for the new assignment.
OS	Select the correct operating system from the drop-down menu. This operating system must be the same operating system used to capture the applications.
Computer Name Prefix	(Optional) Enter a prefix. Entering a prefix limits access to the applications 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 applications assignment regardless of the desktop assignments they are logged in to.

5 Click **Next**.

6 In the New Application dialog box, select the check box next to each application bundle to include in the assignment, and click **Next**.

7 In the **Active Directory Search** text box, start typing the name of a group from your Active Directory.

8 Select a group from the list.

9 (Optional) Search for and select additional groups and click **Next**.

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

The assignment appears on the Assignments page.

11 On the Assignments page, click the new assignment to view details.

What to do next

After you create an application assignment, you can manage the assignment, such as by viewing, editing, or deleting it. See Chapter 7, "Managing Assignments," on page 63.

Working with Writable Volumes 6

Create writable volumes to maintain information about user-installed applications between login sessions. Writable volumes are containers for persistent user-installed applications. After you create a writable volume assignment for a user or group, the corresponding writable volume is created in the datastore in your Horizon Cloud Node environment.

For users, the writable volume is created when you create the assignment using the Administration Console. For groups, the writable volume is created at the user's first login, which slightly increases the amount of time required for the initial login.

- A writable volume is attached to a desktop at user login. When the user logs out, the writable volume is unmounted and detached from the desktop virtual machine.
- Users can have more than one writable volume assigned to them. However, a user can attach only one writable volume to each virtual machine. A writable volume is created for each operating system and desktop prefix combination, and is available only for a single desktop instance with this combination. The writable volume is still in use if a user has an active or disconnected session using that writable volume. If the user attempts to log in to other desktops with the same operating system type and desktop prefix combination, the writable volume does not attach to the new virtual machine.

Writable Volumes FAQ

- I cannot see the writable volume on my additional desktop.

  To avoid conflict and to ensure error-free operation, writable volumes are enabled for one session per user for a given desktop OS type. To enable access to a writable volume on an additional desktop, first log out from any existing connected or disconnected sessions before you log in to the additional desktop.

- How can I check the use and free capacity of my allotted writable volume?

  You can check this information in the Administration Console. Select **Settings > Storage Management** and click **Writable Volumes**.

- How can I get persistence of users' data, settings, and profiles between login sessions?

  To get persistence of users' data, settings, and profiles between login sessions, you must configure your environment according to the best practices described in the VMware App Volumes with Horizon Cloud Application Delivery Best Practices and Operations Procedures document available at vmware.com. That document describes how to leverage User Environment Manager to achieve user settings and persistence management for the virtual desktops and applications delivered by your environment.

This chapter includes the following topics:

Create a Writable Volume Assignment

You can create writable volume assignments to provide users with desktop sessions in which their user-installed applications persist. A writable volume assignment provides a user with an assigned persistent virtual disk where information about the applications they install during their session is kept for use in future sessions.

Procedure

1 In the Administration Console, click **Assign**.

2 Click **New**.

3 In the New Assignment dialog box, click **Get Started** for the Writable Volumes Assignments option.

4 Provide the required information to configure the writable volume assignment.

Option	Description
Assignment Name	Unique name for this new assignment.
OS	Select the correct operating system from the drop-down menu.
Computer Name Prefix	(Optional) The prefix limits the desktop to which the writable volume attaches. The writable volume attaches to the first desktop the user logs in to.
Type	Default type is **UIA** for user-installed applications. Applications that users install appear on the desktop across sessions.
Size	Specify the size of the writable volume in GB. The default size of a writable volume is 5 GB. You can change this default value while creating the writable volume, but not after.

5 Click **Next**.

6 In the **Active Directory Search** text box, start typing the name of a user or group from your Active Directory.

7 Select a user or group from the list.

8 Search for and select additional users or groups, and click **Next**.

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

The new writable volumes assignment appears on the Assignments page. You can click the new writable volumes assignment to view its details.

What to do next

After you create a writable volume assignment, you can manage the assignment, such as viewing, editing, or deleting it. See Chapter 7, "Managing Assignments," on page 63. If you delete a writable volume assignment using the Assignments page, you should also delete the underlying writable volume from the system using the Storage Management page. See "Delete a Writable Volume," on page 61.

Delete a Writable Volume

Use the Administration Console to delete writable volumes from the internal datastore of your Horizon Cloud with On-Premises Infrastructure environment.

Prerequisites

Confirm that the writable volume assignments attached to a virtual machine are no longer needed.

Note Deleting a writable volume permanently erases all the data on it. You cannot recover a deleted writable volume.

Procedure

1 In the Administration Console, select **Settings > Storage Management**.

2 Click **Writable Volumes**.

3 Select the check box next to each writable volume you want to delete.

4 Click **Delete** on the Storage Management page and again in the confirmation dialog box.

Managing Assignments 7

After you create a desktop, application, or writable volume assignment, you can manage the assignment with the Administration Console.

You can view, edit, and delete any of the assignment types. You can recover desktop assignments. For information about creating assignments, see the respective instructions.

- "Create a Dedicated or Floating Desktop Assignment," on page 39
- "Create an Application Assignment," on page 57
- "Create a Writable Volume Assignment," on page 60

This chapter includes the following topics:

View an Assignment

Use the Assignments page to get an overview or detailed view of all the assignment types. You can view the details of individual assignments by clicking the respective assignment. After clicking on a desktop assignment, you can also navigate to its Desktops page where you can perform actions on the individual virtual desktops in that assignment.

Procedure

1 In the Administration Console, open the Assignments page by clicking **Assign**.

2 On the Assignments page, click the name of an assignment to see detailed information.

The assignment opens to its Summary page. The information available is specific to each assignment type.

3 Navigate through the information depending on the assignment type.

Assignment Type	Description
Desktop	View the information on the Summary page and click **Desktops**, **System Activity**, or **User Activity** to view the information on those respective pages or work with the virtual desktops. ■ The Summary page provides definition information about the assignment, the name of an image from which the desktop was created, and a list of the assigned users. ■ The Desktops page provides information about the individual desktops created as part of the desktop assignment. You can also perform actions on an individual desktop, depending on its current state. For example, if a desktop is hung, you can try to reset it. You can also manage the individual desktops in a desktop assignment on the Desktops page. ■ The Activity page provides activity information for that assignment over a specified time.
Application	■ The Summary page provides definition information about the AppStack, a list of the applications in the AppStack, and a list of the assigned users. ■ The Sessions page provides session information for that AppStack.
Writable Volume	View the information on the Summary page. The page includes definition information about the writable volume and a list of the assigned users.

Edit an Assignment

You can edit any assignment type from the Assignments page.

For desktop, application, or writable volume assignments, you can change the name of the assignment or you can add or delete users or user groups. For application assignments, you can add or delete applications.

Procedure

1 In the Administration Console, click **Assign**.

2 Select the check box next to the assignment you want to edit and click **Edit**.

3 Edit the assignment according to type.

Assignment Type	Instructions
Desktop	**Note** If you edit the capacity of a desktops assignment, it takes a few minutes for the system to reflect the change. a On the Definition page of a desktop assignment, edit the settings you want to change and click **Next**. b On the Users page, add or remove users or groups and click **Next**. c Review the Summary page and click **Submit**.
Application	a On the Definition page of an application assignment, edit the settings you want to change and click **Next**. b On the Applications page, select the check box next to each application bundle you want to add or remove and click **Next**. c On the Users page, add or remove user groups and click **Next**. d Review the Summary page and click **Submit**.
Writable Volume	a On the Definition page of a writable volume assignment, edit the name if you want to change it and click **Next**. b On the Users page, add or remove users or groups and click **Next**. c Review the Summary page and click **Submit**.

Resizing a Desktop Assignment

When you create desktop assignments, you assign an initial capacity of desktops. As the user population changes, you might need to expand or shrink a desktop assignment. You can expand an assignment to add additional desktops. You can shrink an assignment to free up capacity to be used elsewhere, for example, when users no longer need to access those resources. The method for increasing and decreasing desktop assignment capacity varies depending on whether the desktop assignment type is floating or dedicated.

Increasing Capacity

Increasing the capacity of a desktop assignment refers to adding desktops to the assignment. You can add desktops by editing the desktop assignment, floating or dedicated, to increase the **Capacity** setting. See "Edit an Assignment," on page 64. You can expand an assignment up to the maximum hardware capacity of your Horizon Cloud Node. After you make the changes, the system starts creating the new desktops. Progress can be monitored from the **Desktops** and **Activity** tabs of the desktop assignment. See "View an Assignment," on page 63.

Decreasing Capacity

The method to decrease capacity varies depending on the desktop assignment type.

Desktop Assignment Type	Description
Floating Desktop Assignment	To reduce a floating desktop capacity, edit the desktop assignment and change the capacity to the new, smaller, number. The system starts to delete desktop virtual machines that are not needed. If the new requested capacity is smaller than the number of available desktops due to users being currently logged on or because they have disconnected sessions, the assignment reduction is prevented and an error message appears. To shrink the assignment in this situation, you must first wait for, or force, the users to fully logoff, before you adjust the pool capacity. Alternatively, you can shrink the capacity by a smaller amount to remove any currently unused desktops.
Dedicated Desktop Assignment	Because dedicated desktop assignments are mapped to specific users when they first connect, you cannot simply reduce the capacity of the assignment. Such an action would not provide instructions to the system about which desktops to delete. To reduce the size of the dedicated assignment, from the **Desktops** tab, select the check box next to the desktops you want to delete. You can delete desktops that are unassigned or desktops that have been assigned to a specific user. Then select **… > Delete**. A confirmation dialog box appears. After you delete the desktops, the assignment size automatically decreases. You do not need to edit the pool settings to reduce the desktop assignment size. **Note** You cannot delete a desktop that has an active, or disconnected, session. Users must be fully logged off before you can delete the desktop. If you want the desktop to be used by another user, but want to keep the same capacity, you can select the check box next to the desktop and select **… > Unassign**.

Delete a Desktop Assignment

You can delete a desktop assignment that is no longer needed.

The system does not allow you to delete a desktop assignment that is in use.

Prerequisites

Decrease the capacity of the desktop to zero. See "Decreasing Capacity," on page 65. The capacity of an assignment must be zero before you can delete the assignment.

Procedure

1 In the Administration Console, click **Assign**.

2 Select the desktop assignment to delete and click **Delete**.

3 Click **Delete** in the confirmation dialog box to permanently delete the assignment.

Delete an AppStack Application or Writable Volume Assignment

You can delete an AppStack application or writable volume assignment that is no longer needed.

The system does not allow you to delete an AppStack application or writable volume assignment that is in use.

Procedure

1 In the Administration Console, click **Assign**.

2 Select the AppStack application or writable volume assignment to delete and click **Delete**.

3 Click **Delete** in the confirmation dialog box to permanently delete the assignment.

The result differs depending on if the assignment is an AppStack application assignment or a writable volume assignment.

Assignment Type	Result
AppStack application	Users lose access to the applications at their next login.
Writable volume	Users continue to experience persistence of their installed applications on their desktops across sessions as provided by the writable volume assignment until you delete the writable volume.

What to do next

To delete a writable volume, see "Delete a Writable Volume," on page 61.

Recover Desktops in a Desktop Assignment

If desktops in an assignment encounter errors during a previous image update or re-sync, or if they do not power back on after an image update or re-sync, use the recover action on the desktop assignment.

Procedure

1 In the Administration Console, click **Assign**.

2 Select the desktop assignment to recover.

3 Click **Recover** on the Assignments page and again in the confirmation dialog box.

Integrate Horizon Cloud with On-Premises Infrastructure with a VMware Identity Manager Environment

8

By integrating your Horizon Cloud with On-Premises Infrastructure environment with an on-premises or cloud-hosted VMware Identity Manager™ environment, you give your VMware Identity Manager users the ability to access their entitled desktops using the Workspace ONE portal.

VMware Identity Manager is an Identity as a Service (IDaaS) offering that provides application provisioning, a self-service catalog, conditional access controls, and single sign-on (SSO) for SaaS, web, cloud, and native mobile applications. VMware Identity Manager is available both as an on-premises product and as a service hosted by VMware.

For an overview of this integration from the perspective of the VMware Identity Manager environment, see the Providing Access to Horizon Cloud overview. You configure desktop assignments for your users and groups in the Horizon Cloud Administration Console as usual. After you complete the steps to integrate the Horizon Cloud Node environment with your VMware Identity Manager environment, you sync the desktop assignment information to the VMware Identity Manager service. Then you can see the desktops in the VMware Identity Manager administration console and your end users can access their desktops from the Workspace ONE portal. You can set up a regular sync schedule to sync the assignment information from your Horizon Cloud Node environment to your VMware Identity Manager environment.

Note When you integrate VMware Identity Manager with Horizon Cloud with On-Premises Infrastructure, a best practice is to include Unified Access Gateway in the configuration to provide your end users with seamless HTML web access to their virtual desktops. See the Unified Access Gateway product documentation for deployment steps.

The following list is a high-level summary of the end-to-end steps to enable your end users to access their entitled desktops using the Workspace ONE portal.

1. Obtain a VMware Identity Manager environment, either by deploying the on-premises version or by subscribing to the cloud-hosted version.
2. Deploy VMware Identity Manager according to the VMware Identity Manager guidelines for the deployment model you are using.

   If you are using the cloud-hosted VMware Identity Manager, you must install a VMware Identity Manager connector appliance on premises in your Active Directory network. For details, see the description of the deployment scenario in the VMware Identity Manager documentation.
3. Ensure that you meet the VMware Identity Manager prerequisites for integration, as documented in the VMware Identity Manager product information appropriate for your situation:

VMware Identity Manager environment	Prerequisites
Cloud-hosted	Prerequisites for Integration
On-premises version 2.8.x	Prerequisites for Integration

4 Install certificates into your VMware Identity Manager environment and your Horizon Cloud Node environment.

5 Enable desktops from your Horizon Cloud with On-Premises Infrastructure environment to the VMware Identity Manager environment, as documented in the VMware Identity Manager product information appropriate for your situation:

VMware Identity Manager environment	Link to Desktop Enablement Documentation
Cloud-hosted	Enable Horizon Cloud Desktops and Apps in VMware Identity Manager
On-premises version 2.8.x	Enable Horizon Cloud Desktops and Apps in VMware Identity Manager

6 In your VMware Identity Manager environment, configure a federation artifact for your Horizon Cloud with On-Premises Infrastructure environment. The federation artifact is needed for configuration of the SAML authentication between the two environments. See "Configure VMware Identity Manager for Horizon Cloud with On-Premises Infrastructure," on page 69.

7 Configure Horizon Cloud with On-Premises Infrastructure for VMware Identity Manager access. See "Configure Horizon Cloud Node for VMware Identity Manager," on page 70.

8 In your VMware Identity Manager environment, sync the entitled desktops to VMware Identity Manager, as documented in the VMware Identity Manager product information appropriate for your situation:

VMware Identity Manager environment	Link to Desktop Enablement Steps
Cloud-hosted	Syncing Horizon Cloud Desktops and Apps with VMware Identity Manager
On-premises version 2.8.x	Syncing Horizon Cloud Desktops and Apps in VMware Identity Manager

9 Verify end-user access to desktops by logging in to the Workspace ONE portal as an end user and launching a desktop from the catalog. See "Confirm End-User Access to Desktop Assignments in VMware Identity Manager," on page 72.

Prerequisites

To complete the integration process through the step of verifying end-user desktop access using the Workspace ONE portal, ensure that you have the following items.

- A fully configured Horizon Cloud Node environment, that uses trusted certificates and has configured desktop assignments. For steps on uploading certificates to your Horizon Cloud Node, see "Upload Certificates," on page 23.
- Access to your organization's configured VMware Identity Manager environment, either an on-premises or a cloud-hosted environment. Your VMware Identity Manager environment must be configured with trusted certificates.

  If you are deploying VMware Identity Manager on premises, follow the deployment information in the VMware Identity Manager documentation center for your version of the on-premise product. The documentation centers for each on-premise product version are available from the VMware Identity Manager documentation page. For the specific versions of the on-premises VMware Identity Manager product that are supported for use with this version of Horizon Cloud with On-Premises Infrastructure, see the *Release Notes*.

  If you are using the cloud-hosted VMware Identity Manager, you must install a VMware Identity Manager connector appliance on premises in your Active Directory network. Follow the steps as documented in the VMware Identity Manager documentation center, and see the description of this deployment scenario and subtopics. For the connector version that is required for this release of Horizon Cloud with On-Premises Infrastructure, see the *Release Notes*.

Verify that your configured VMware Identity Manager environment meets the prerequisites for integration with Horizon Cloud resources, as described in the VMware Identity Manager documentation.

VMware Identity Manager environment	Prerequisites
Cloud-hosted	Prerequisites for Integration
On-premises version 2.8.x	Prerequisites for Integration

Optionally integrate Unified Access Gateway with Horizon Cloud with On-Premises Infrastructure. Using Unified Access Gateway in this configuration is a best practice. See the deploying and configuration information available at the Unified Access Gateway, in the Unified Access Gateway product documentation available at its Unified Access Gateway documentation landing page.

Procedure

1 Configure VMware Identity Manager for Horizon Cloud with On-Premises Infrastructure on page 69

To integrate Horizon Cloud with On-Premises Infrastructure with VMware Identity Manager, you must configure VMware Identity Manager with Horizon Cloud Node information. This process configures the federation artifact in your VMware Identity Manager environment for Horizon Cloud with On-Premises Infrastructure. The federation artifact is needed for the SAML authentication.

2 Configure Horizon Cloud Node for VMware Identity Manager on page 70

To integrate your Horizon Cloud with On-Premises Infrastructure environment with your VMware Identity Manager environment, you must configure your Horizon Cloud Node with the appropriate VMware Identity Manager information. You use the Administration Console to configure this information.

3 Confirm End-User Access to Desktop Assignments in VMware Identity Manager on page 72

After you integrate Horizon Cloud with On-Premises Infrastructure with a VMware Identity Manager on-premises deployment, you can confirm that end users have remote access to their virtual desktops.

What to do next

After you have verified the integration is working, you can optionally enforce end users to access their desktops using VMware Identity Manager. See "Enforce End-User Access Through VMware Identity Manager," on page 96.

Configure VMware Identity Manager for Horizon Cloud with On-Premises Infrastructure

To integrate Horizon Cloud with On-Premises Infrastructure with VMware Identity Manager, you must configure VMware Identity Manager with Horizon Cloud Node information. This process configures the federation artifact in your VMware Identity Manager environment for Horizon Cloud with On-Premises Infrastructure. The federation artifact is needed for the SAML authentication.

Prerequisites

Verify that you have met the prerequisites described in Chapter 8, "Integrate Horizon Cloud with On-Premises Infrastructure with a VMware Identity Manager Environment," on page 67.

If you are not using Unified Access Gateway, obtain the FQDN used for your Horizon Cloud Node, such as `desktops.mycorp.com`. One way to obtain the FQDN is to first locate the IP address in the Administration Console by navigating to **Settings > Infrastructure**. Then obtain the FQDN that is associated with that IP address from your organization's DNS information.

Note If you are using an on-premises VMware Identity Manager environment, using the Horizon Cloud Node IP address instead of its FQDN technically works. However, that configuration is not recommended.

If you are using Unified Access Gateway, obtain the URL used for your Unified Access Gateway deployment.

Procedure

- In the VMware Identity Manager administration console, configure the federation artifact settings for Horizon Cloud as described in the VMware Identity Manager documentation.

Setting	Description
Assertion Consumer Service	Type the URL to which the SAML assertion is to be posted. The URL must be one of the following items, depending on your installed environment: ■ The Unified Access Gateway URL, if you are using Unified Access Gateway ■ A URL of the form `https://`*`Node-FQDN`* where *Node-FQDN* is the FQDN of your Horizon Cloud Node, such as `http://ournode-sm1.example.com`.
Audience	This setting is a unique identifier for your environment that you are integrating with VMware Identity Manager. You typically use the same URL as used in the **Assertion Consumer Service** field, either the Unified Access Gateway URL or a URL constructed from the Horizon Cloud Node FQDN. This field corresponds to the AudienceRestriction condition in SAML authentication, which describes the context in which the SAML assertion is valid. Your Unified Access Gateway or Horizon Cloud Node uses this property to verify that it is the intended recipient of the SAML response from VMware Identity Manager.
Tenant Appliance URLs	Type an `admin/SAML/metadata` URL of one of the following forms, depending on your installed environment. ■ If you are using Unified Access Gateway, type a URL of the form `https://`*`UnifiedAccessGateway-FQDN`*`/admin/SAML/metadata` where *UnifiedAccessGateway-FQDN* is the FQDN of your Unified Access Gateway. ■ If you are not using Unified Access Gateway, type a URL of the form `https://`*`Node-FQDN`* where *Node-FQDN* is the FQDN of your Horizon Cloud Node.

What to do next

Configure the identity provider information needed for the SAML authentication in your Horizon Cloud with On-Premises Infrastructure environment. See "Configure Horizon Cloud Node for VMware Identity Manager," on page 70.

Configure Horizon Cloud Node for VMware Identity Manager

To integrate your Horizon Cloud with On-Premises Infrastructure environment with your VMware Identity Manager environment, you must configure your Horizon Cloud Node with the appropriate VMware Identity Manager information. You use the Administration Console to configure this information.

You use the General Settings page to configure the VMware Identity Manager information.

Prerequisites

Verify that you have completed the steps to configure the federation artifact as described in "Configure VMware Identity Manager for Horizon Cloud with On-Premises Infrastructure," on page 69.

Verify that you have the following information:

- The SAML identity provider (IdP) metadata URL from your VMware Identity Manager environment. You obtain the environment's SAML IdP metadata URL using the VMware Identity Manager administration console and navigating to **Catalog > Settings > SAML Metadata**. When you click the **Identity Provider (IdP) metadata** link on that page, your browser's address bar displays the URL, typically in the form `https://VMwareIdentityManagerFQDN/SAAS/API/1.0/GET/metadata/idp.xml`, where *VMwareIdentityManagerFQDN* is the fully qualified domain name (FQDN) of your VMware Identity Manager environment. For details, see the VMware Identity Manager product information appropriate for your situation:

VMware Identity Manager environment	Configure SAML Authentication Steps
Cloud-hosted	Configure SAML Authentication in the Horizon Cloud Tenant
On-premises version 2.8.x	Configure SAML Authentication in the Horizon Cloud Tenant

- If you are not using Unified Access Gateway, obtain the FQDN used for your Horizon Cloud Node, such as `desktops.mycorp.com`. One way to obtain the FQDN is to first locate the IP address in the Administration Console by navigating to **Settings > Infrastructure**. Then obtain the FQDN that is associated with that IP address from your organization's DNS information.
- If you are using Unified Access Gateway, obtain the URL used for your Unified Access Gateway deployment.

Procedure

1 Log in to the Administration Console at https://cloud.horizon.vmware.com.

2 Navigate to **Settings > General Settings** and click **Edit**.

3 In the IDM section, click **Add IDM**.

4 Configure the following options.

Setting	Description
IDM URL	Type your VMware Identity Manager environment's SAML IdP metadata URL, typically of the form `https://VMwareIdentityManagerFQDN/SAAS/API/1.0/GET/metadata/idp.xml` where *VMwareIdentityManagerFQDN* is the FQDN of your VMware Identity Manager environment.
Timeout SSO Token	(Optional) The amount of time, in minutes, after which the SSO token times out. The default is zero (0).
Data Center	The drop-down displays a numeric indicating the build version of the installed Horizon Cloud Node software.
Tenant Address	Type one of the following items, depending on whether you are using Unified Access Gateway in this integration: ■ The FQDN for your Horizon Cloud Node. ■ The FQDN for your Unified Access Gateway deployment. **Important** This value must correspond to the settings that you configured in the corresponding federation artifact in the VMware Identity Manager environment, either using the Horizon Cloud Node information or the Unified Access Gateway information.

5 Click **Save**.

A status of green indicates that the configuration is successful.

What to do next

In your VMware Identity Manager environment, sync the entitled desktops to VMware Identity Manager, as documented in the VMware Identity Manager product information appropriate for your situation:

VMware Identity Manager environment	Link to Desktop Enablement Steps
Cloud-hosted	Syncing Horizon Cloud Desktops and Apps with VMware Identity Manager
On-premises version 2.8.x	Syncing Horizon Cloud Desktops and Apps in VMware Identity Manager

Confirm End-User Access to Desktop Assignments in VMware Identity Manager

After you integrate Horizon Cloud with On-Premises Infrastructure with a VMware Identity Manager on-premises deployment, you can confirm that end users have remote access to their virtual desktops.

Prerequisites

Configure the methods of access you want to provide end users with to access desktops through VMware Identity Manager.

Ensure that the entitled desktops are synced from your Horizon Cloud Node to your VMware Identity Manager environment. Follow the steps documented in the VMware Identity Manager product information appropriate for your situation:

VMware Identity Manager environment	Link to Desktop Enablement Steps
Cloud-hosted	Syncing Horizon Cloud Desktops and Apps with VMware Identity Manager
On-premises version 2.8.x	Syncing Horizon Cloud Desktops and Apps in VMware Identity Manager

Procedure

1 Use your organization's VMware Identity Manager URL to log in to the Workspace ONE portal.

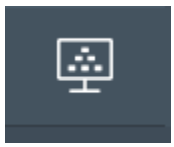
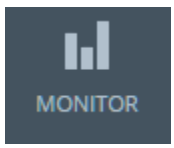
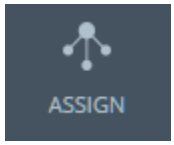
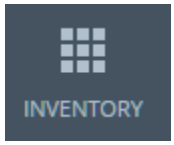
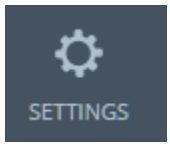
2 Launch entitled Horizon Cloud with On-Premises Infrastructure desktops from the portal.

About Menu Selections in the Administration Console

9

The menu icons provide a quick way to navigate to monitor activity and perform various functions in your Horizon Cloud with On-Premises Infrastructure environment. The icons are located along the left side of the Administration Console.

Table 9-1. Administrator Functions

Icon	Selection	Description
	Dashboard	Displays the Dashboard screen, where you can get a top-level view of the state of your envirionment.
	Monitor	Provides access to dashboards for monitoring desktop information, administrator and user activity, user and desktop mapping, and notifications.
	Assign	Opens the Assignments screen from which you can work with assignments for desktops, AppStacks, and user writable volumes.
	Inventory	Work with the AppStacks and virtual machines (VMs) that were imported from the file share registered with the Horizon Cloud Node. Work with desktop images.
	Settings	Open screens from which you can work wtih system-wide settings and configurations for: ■ Active Directory domains ■ Roles and permissions ■ Utility VMs ■ Two-factor authentication ■ Locations ■ Storage management ■ Infrastructure ■ Getting Started wizard

This chapter includes the following topics:

About the Monitor Icon

Use the **Monitor** icon to navigate to dashboards where you can view information about administrator and user activity in the environment, see system notifications, and view reports that show relationships between users and desktops.

Click the **Monitor** icon to navigate to these pages.

Option	Description
Dashboard	Displays details about desktop connections, connection states, Horizon Cloud Node heath status, and capacity allocation.
Activity	Displays activity details for administrators and end users.
Reports	Provides mapping details for users and desktops.
Notifications	Lists notifications, which provide information about the system, such as important events.

Dashboard Page

This page is available from the **Monitor** icon and displays statistical information about connections and desktop capacity allocation. You can see statistical information for various categories.

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

Category	Description
Appliances	The health status of the Horizon Cloud Node.
Connections	Number of connected sessions, by assignment type.
Connection States	Number of connected sessions, by status: active, idle, disconnected.
Capacity	Desktop and disk space capacity in use, and total allocated desktops by their desktop model type.

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

Column	Description
Description	Details regarding the event.
% Completion	Current percentage of event completed.
Status	Successful indicates an event was performed in its entirety. Failed indicates an event was either partially performed or not performed at all.
Time	Time that the event was logged.

User Events

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

Column	Description
Description	Details regarding the event.
Time	Time that the event was logged.

Reports Page

The Reports page shows information about the relationships between users and desktops in the system.

The Reports page is available from the **Monitor** icon. The page provides the following information.

Mapping Type	Details
User Mapping	View details about the relationships between end users and their assignments.
Desktop Mapping	View details about the relationships between desktop images and other information, such as the assignment names, assigned users and user groups, and so on.

You can also manually refresh this page, filter your search, and export data to a Microsoft Excel worksheet.

Notifications Page

The Horizon Cloud with On-Premises Infrastructure environment uses notifications to inform you of certain types of system activity, such as events and service registrations.

You can view recent notifications in the Administration Console by clicking the bell icon located in the upper right corner of any page () Open the Notifications page to view all notifications, which includes both active and dismissed notifications, by clicking **Monitor > Notifications**.

You can also show the notifications for different periods of time up to 30 days, refresh the page, and filter your search.

Table 9-2. Notification Types

Notification Type	Description
File Share Import	A file share import notification informs you that the file share import process either failed or succeeded. The file import process pulls application data from a shared file store into the Horizon Cloud with On-Premises Infrastructure environment.
Service Registration	Service registration notifications are issued during the configuration of Horizon Cloud with On-Premises Infrastructure. The system issues this type of notification when a packaged service is registered successfully. The packaged services are APPVOLUMES and DAAS.

About the Assign Icon

The **Assign** icon displays the Assignments page, where you can create and work with assignments in your Horizon Cloud with On-Premises Infrastructure environment.

Action	Description
New	Create assignments for desktops, AppStacks, and writable volumes.
Edit	Use this button to modify characteristics of the selected assignment.
Delete	Use this button to delete the selected assignment.
Recover	Use this button to recover desktops that encountered an error during the previous image update. Available for desktop assignments.

For each assignment, you can click its name see more information about that assignment, such as which users it is assigned to and other details.

When you click on a desktop assignment, in addition to seeing more information about the assignment, you can also navigate to the desktop assignment's Desktops tab to see the list of virtual desktops that are in that desktop assignment and optionally perform actions on those desktops.

For detailed information about managing assignments in the environment, see Chapter 7, “Managing Assignments,” on page 63.

About the Inventory Icon

Use the **Inventory** icon to navigate to pages where you can work with desktop images, view the AppStacks and master virtual machines (VMs) that have been imported into the environment from the registered file shares, and convert the master VMs into desktop images.

Click the **Inventory** icon to navigate to these pages.

Option	Description
Applications	Opens the Applications page, where you can view, hide, or rename the imported AppStacks.
Images	Opens the Images page. At a page level, you can: ■ View the desktop images available in the system. ■ Create a desktop image. ■ Download the DaaS bootstrap file ■ Refresh the DaaS bootstrap password When you select the check box for a specific desktop image, you can perform the following actions on it: ■ Rename, duplicate, delete it. ■ Convert to a desktop. ■ Assign it to an existing desktop assignment. See Chapter 4, "Creating Desktop Assignments," on page 35.
Imported VMs	Opens the Imported VMs page where you can view a list of virtual machines that the system imported from the OVAs on the file share registered with your Horizon Cloud Node. You can move VMs from this page to the Utility VMs page, according to your organization's needs. See "Imported VMs Page," on page 77.

Imported VMs Page

The Imported VMs page in the Administration Console lists the master virtual machines (VMs) that the system imported into the Horizon Cloud Node from the OVAs on the connected file share. Only VMs that have Microsoft Windows guest operating systems are imported.

You can perform the following actions on the listed VMs by selecting the check box next to the VM and clicking the respective action.

Action	Description
Rename	Rename the selected VM.
VM power and guest operating system actions	Depending on the current state of the VM, these standard VM power operations are available: power on, power off, suspend, reset. Operations on the guest operating system are: logoff, disconnect, restart, shutdown.
Delete	Delete the selected VM.
Migrate to Utility VMs	Move the VM to the Utility VMs page. See "Utility VMs Page," on page 80
Convert to Image	Convert the selected VM to a desktop image that the system can use to spin out the virtual desktops. The VM must have the agents installed and configured and meet the requirements as described in Chapter 3, "Creating a Desktop Image," on page 25.

About the Settings Icon

You use the **Settings** icon to navigate to pages for working with general settings, working with roles and persmissions, working with utility virtual machines (VMs), uploading certificates, managing storage-related items, configuring two-factor authentication, and working with settings related to the deployed Horizon Cloud Node environment.

Click the **Settings** icon to access these pages in the Administration Console.

User Interface Page	Description
General Settings	Displays settings for networks, domains, and so on. You can edit settings from this page, and upload certificates. See "Edit General Settings," on page 78 for details.
Active Directory	View and edit Active Directory details. See "Register Your First Active Directory Domain with Your Horizon Cloud Node," on page 12 for details.

User Interface Page	Description
Roles & Permissions	Edit roles and permissions. See "Assign Roles to Users for Administration Console Access," on page 24.
Utility VMs	Displays virtual machines (VMs) that are used for infrastructure services like DHCP. Usually a VM is listed on this page when you have moved it from the Imported VMs page. See "Utility VMs Page," on page 80.
Locations	Displays details about your environment's App Volumes Manager instance, the vCenter Server instance, and configured file share. You can work with the configured file share from this page. See "Locations Page," on page 80.
Storage Management	Delete AppStacks or writable volumes from the datastore, for example to clean up disk space.
Infrastructure	View details about the deployed Horizon Cloud Node environment such as its location, type, desktop models, remaining capacity, and IP addresses. You can also edit the name and description of the Horizon Cloud Node. See "Infrastructure Page," on page 81.
Getting Started	Opens the Getting Started wizard. See "Getting Started Wizard for Your Horizon Cloud Node Environment," on page 16 for details.
2 Factor Auth	Configure two-factor authentication for end users. See "Configuring Two-Factor Authentication for Your Horizon Cloud with On-Premises Infrastructure Environment," on page 82.

Edit General Settings

Use the General Settings page to modify general settings and upload certificates for your Horizon Cloud Node instance.

Procedure

1 Select **Settings > General Settings**.

2 Click **Edit**.

3 Make changes for these settings.

Option	Description
Default Domain	Default domain that you are editing.
Session Timeout	Assign or change the timeout setting for each portal.
Image Defaults Configuration	If you require a desktop image to be registered against an OU in Active Directory other than CN=Computers, enter the value in the **Image OU** text box.
User Portal Configuration	Enter the help desk email address, the trouble ticket system URL, and the external style sheet URL for the end-user portal configuration.
User Account Configuration	When you have the **IDM** settings configured for at least one VMware Identity Manager environment, these two options are available to enforce use of the Workspace ONE portal for desktop access: ■ Set **Force Remote Users to vIDM** to **Yes** to require users outside your corporate network to use the Workspace ONE portal to access their desktops. ■ Set **Force Internal Users to vIDM** to **Yes** to require users inside your corporate network to use the Workspace ONE portal to access their desktops.

Option	Description
IDM	Click **Add IDM** as part of integrating this Horizon Cloud Node with a VMware Identity Manager environment. This information configures the VMware Identity Manager Complete the displayed form for the following information: ■ URL of your VMware Identity Manager environment. ■ Optionally provide the timeout, in minutes, for the SSO tokens. These SSO tokens are used to enforce this timeout for your end users. ■ Select the data center for which you are configuring the use of the VMware Identity Manager environment. ■ Type the Horizon Cloud Node IP address that is used for desktop access.
HTML Access	The **Cleanup credentials when tab is closed** setting affects system security and ease of use when end users access desktops or applications using HTML Access. The setting determines if end users must re-enter their credentials when they reconnect. ■ A value of **Yes**, the option that emphasizes security, prompts end users to re-enter their credentials. ■ A value of **No**, the option that emphasizes ease of use, does not prompt end users to re-enter their credentials.
Agent Pairing	Sets a policy on your environment which determines the access of desktops that are using legacy (pre-16.6.0) and 16.6.0 agents. ■ The **15.3 Compatibility Mode** option allows pairing of the legacy and 16.6.0 agents with your environment. This option also applies to the 16.3 agents. This option is the default setting for updated environments. ■ Even though the **16.6 Upgrade Mode** option restricts fresh pairings by legacy agents, this mode allows a desktop that is already paired using the 16.3.0 agent unless the desktop or the agent service is restarted. ■ The **16.6 Mode** option allows only bootstrapped 16.6.0 agents to pair with the environment. This mode does not restrict a desktop that is already paired using 16.3.x agents or using unbootstrapped 16.6.0 agents unless the desktop or DaaS agent service is restarted. This option is the default setting for fresh installs.
Contact Info	Administrator contact information

4 Click **Save**.

Session Timeout Settings

Adjust the session timeout settings in Horizon Cloud with On-Premises Infrastructure to allocate enough time to avoid data loss.

Timeout	Description
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 in a connected session. When this maximum is reached, the user is disconnected from all active Horizon Client desktop sessions. The user must reauthenticate to reaccess the Horizon Client. **Note** Set the **Client Idle User** timeout to be at least double the **Client Heartbeat Interval** setting to avoid unexpected disconnects from desktops.

Timeout	Description
Client Broker Session	Maximum time that a Horizon Client instance can be connected to the system environment before the session's 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 reauthenticate 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** setting and the **Client Idle User** timeout.
User Portal Timeout	For a Horizon Cloud with On-Premises Infrastructure environment, this setting is deprecated and has no effect.

Locations Page

The Locations page provides details for your environment's App Volumes Manager, vCenter Server, and the file shares.

Procedure

- Navigate to **Setttings > Locations** to view these details.

Option	Description
AV Manager	Displays details for the App Volumes Manager.
vCenter	Shows details for the Horizon Cloud Node's vCenter Server instance .
File Share	Displays file shares that are registered with your environment. From here you can take the following actions. ■ "Register a File Share," on page 22 ■ "Edit a File Share," on page 80 ■ "Import AppStacks," on page 56

Edit a File Share

You can edit a file share name, source path, and destination vCenter Server instances.

Procedure

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

Utility VMs Page

The Utility VMs page in the Administration Console provides actions for virtual machines (VMs) that you might have added to your environment for infrastructure-related capabilities, such as DHCP, Domain Controller functions, and so on.

You can perform the following actions on the listed VMs by selecting the check box next to the VM and clicking the respetive action.

Action	Description
Rename	Rename the selected VM.
VM power and guest operating system actions	Depending on the current state of the VM, these standard VM power operations are available: power on, power off, suspend, reset. Operations on the guest operating system are: log off, disconnect, restart, shutdown.
Migrate to Imported VMs	Move the VM to the Imported VMs. See "Imported VMs Page," on page 77.

Infrastructure Page

On the Infrastructure page, you can view and edit details such as status, location, and Horizon Cloud Node IP address for a deployed Horizon Cloud Node environment. The Infrastructure page is available from the **Settings** icon.

Table 9-3. Horizon Cloud Node Environment Details Available from the Infrastructure Page

Environment Details	Description
Details about the Horizon Cloud Node installed virtual appliance	By default, the Infrastructure page displays the status, name, location, type, and assigned IP address from the desktop network. **Note** This IP address was formerly referred to as the tenant appliance IP address or tenant IP address. You might see the labels in the Administration Console reflecting that prior name. You can view the management and desktop networking information by selecting the checkbox next to the listed Horizon Cloud Node and clicking **Edit**. In the Edit window, you can optionally customize the name, location, and description.
Details about the desktops	You can view details about the environment's virtual desktops by clicking the name in the Appliance column. ■ In the Summary section, you can see appliance status, location, total number of allocated desktops, and available desktop capacity. Place the cursor over these values to see further details for each. You can also see the available disk space capacity and number of active sessions. ■ The Summary also shows the current software version running in the appliance, and whether an update is available. Clicking the software version hyperlink displays a window that describes the most recent features provided in that version. ■ The Allocated Desktop Model section displays a list of the desktop models that are provided in a Horizon Cloud with On-Premises Infrastructure environment, details about each one, and the number allocated for each type.

Determine the Horizon Cloud Node IP Address for Use by Desktops

During deployment, the Horizon Cloud Node appliance is assigned two IP addresses: one from the management network and one from the desktop network. The Horizon Cloud Node IP address that is assigned from the desktop network is used for DaaS Agent, Horizon Client, and HTML Access configuration and for building a master virtual machine for the desktop image.

Note This IP address was formerly referred to as the tenant appliance IP address or tenant IP address. You might see the labels in the Administration Console reflecting that former name.

Procedure

1 In the Administration Console, select **Settings > Infrastructure**.

2 Create a DNS record for the Horizon Cloud Node IP address, for example, `myDesktops.myCorp.com`.

This address becomes the server address that end users use when they use the Horizon Client or HTML Access to access their desktops.

Configuring Two-Factor Authentication for Your Horizon Cloud with On-Premises Infrastructure Environment

For two-factor authentication of end users that are internal on your corporate network, you can use RSA SecurID or RADIUS (Remote Authentication Dial-In User Service) server authentication. For two-factor authentication of end users that are external to your corporate network, you configure Unified Access Gateway to provide that authentication.

To enable two-factor authentication for end users that are connecting to their assigned resources from outside of the corporate network, you configure authentication when you deploy and configure Unified Access Gateway for use with your installed environment. For the steps on deploying and configuring Unified Access Gateway, see the Unified Access Gateway product information at www.vmware.com/support/pubs/.

To configure the settings for two-factor authentication for your end users that are connecting to their assigned resources from within your internal corporate network, use the 2Factor Authentication page in the Administration Console.

Prerequisites

Install and configure the two-factor authentication software, either the RSA SecurID software or the RADIUS software, on an authentication manager server.

When using RSA SecurID authentication, export the `sdconf.rec` configuration file from your RSA Authentication Manager. You upload this file when configuring RSA SecurID two-factor authentication using the Administration Console.

When using RADIUS authentication, verify you have the following required information from your RADIUS server installation. These values are required when configuring RADIUS two-factor authentication using the Administration Console.

- RADIUS server's DNS name or IP address
- If different from the default port of 1812, the UDP port number on which the RADIUS server is listening for RADIUS authentication
- The authentication type, such as PAP, CHAP, MS-CHAPv1, or MS-CHAPv2
- The shared secret

Important Before using the Administration Console to configure the settings for two-factor authentication using RADIUS, make sure that the Horizon Cloud Node IP address is registered as a client on the RADIUS server and auxiliary RADIUS server, if any. Go to **Settings > Infrastructure** to obtain the Horizon Cloud Node IP address. See "Infrastructure Page," on page 81 for details.

Procedure

1 In the Administration Console, select **Settings > 2 Factor Auth**.

2 Click **New**.

3 Select the authentication method.

4 Configure the appropriate settings according to your selected authentication method.

- When using RADIUS authentication:

Setting	Description
Maintain Username	Select **Yes** to force matching of the RADIUS user names with the user names in Active Directory. If you select **Yes**, the user attempting to authenticate must match the RADIUS user name. If you select **No**, the user name is not locked and the user can enter a different name.
Provider Name	(Required) Name that distinguishes the type of RADIUS authentication being used.
Host Name / IP Address	(Required) DNS name or IP address of the authentication server.
Shared Secret	(Required) Secret for communicating with the server. The value must be identical to the server-configured value.
Authentication Port	UDP port configured to send or receive authentication traffic. Default is 1812.
Accounting Port	UDP port configured to send or receive accounting traffic. Default is 1813.
Mechanism	Select the RADIUS authentication protocol: PAP, CHAP, MS-CHAPv1, or MS-CHAPv2.
Server Timeout	Number of seconds to wait for a response from the RADIUS server. Default is five seconds.
Max number of Retries	Maximum number of times to retry failed requests. Default is three tries.
Realm Prefix	Name and delimiter of realm to be prepended to the user name during authentication.
Realm Suffix	Name and delimiter of realm to be appended to the user name during authentication.
Auxiliary Server	Default is **NO**. If set to **YES**, configure the appropriate settings for a secondary RADIUS server to be used when the primary server is not responding.

- When using RSA SecurID authentication:

Setting	Description
Maintain Username	Select **Yes** to force matching of the RSA SecurID user name during authentication. The user attempting to authenticate must have the same user name credentials for RSA and Domain Challenge. If you select **No**, the user name is not locked and the user can enter a different name.
Upload Configuration File	Click **Select** to navigate to and upload the `sdconf.rec` file.

5 Click **Save**.

The Test Authentication windows appears.

6 Enter your user name and passcode in the Test Authentication dialog box, then click **Test**.

The result depends on the outcome of the test authentication:

- If the authentication test is successful, your configuration settings are saved to the system and users attempting to authenticate with the tenant portals will see a dialog box asking them to log in with their credentials, followed by their domain credentials.
- If the Test Authentication credentials fail, the Test Authentication window remains open and your configuration settings are not saved. Correct the user name or passcode and try again or cancel out of the window and verify your configuration settings.

Managing Horizon Cloud Nodes 10

After you install and configure one or more Horizon Cloud Nodes, you can perform tasks to manage them.

For example, you can monitor the health of your Horizon Cloud Nodes, put Horizon Cloud Nodes into maintenance mode, and perform update-related tasks.

For information about logging in to a Horizon Cloud Node, including details about selecting a node to log in to when your environment includes multiple Horizon Cloud Nodes, see "Log in to the Administration Console Used with Horizon Cloud Nodes," on page 14.

This chapter includes the following topics:

Monitor Horizon Cloud Node Health

In the Administration Console, use the Dashboard page to check the health of your Horizon Cloud Node. You navigate to the Dashboard page using the **Monitor** icon.

A Horizon Cloud Node primarily consists of a single virtual appliance deployed into a virtual infrastructure, such as a vSAN Ready Node. On the Dashboard page, the environment is labeled Horizon Cloud Node and an icon next to the label indicates its health:

- Healthy (check mark)
- Warning (exclamation point)
- Faulty (red cross)

The indicated health reflects the status of the environment's underlying software components that provide the services to make the desktops work, such as:

- The component that manages the entire installed environment, providing common services that allow communication between components.
- The component that communicates to the underlying cluster infrastructure such as the vCenter Server and vSphere software, providing the separation from desktop management and infrastructure management.
- The component that provides desktop manager services, manages the instant clone provisioning engine and the desktop broker, and talks to the agents in the virtual desktops.

- The App Volumes Manager component that manages the AppStacks.

If an issue is reported with either the warning or faulty icon, you can click the displayed name to examine the reported details. Certain issues can often be remedied on premise.

For NTP issues, confirm that the NTP servers listed are functional and accessible from the Horizon Cloud Node appliances deployed in the virtual infrastructure.

For Active Directory issues, confirm that the Active Directory server is functional, the service account used by the Horizon Cloud Node to query the Active Directory server is enabled, not locked, and the password has not changed

Certain issues might require additional help from VMware Support. For database replication issues, contact VMware Support for assistance. Such database issues might indicate that the system has failed to backup which can result in restricted functionality.

Procedure

1 In the Administration Console, select **Monitor > Dashboard**.

2 If the Horizon Cloud Node status indicates warning or faulty, click its name for details.

A dialog box appears. The dialog box includes a **more** link. Depending on the health status, the dialog box might list health issues specific to the environment.

3 Click **more**.

4 The page displays more information and guidance. If you want to create a list of the issues, click **Download** to download a spreadsheet that lists the issues for that Horizon Cloud Node.

Perform Maintenance on an ESXi Host in a Horizon Cloud Node

Performing maintenance on a Horizon Cloud Node usually involves putting one of its underlying ESXi hosts into maintenance mode using one of the vSphere clients, such as the vSphere Web Client or vSphere Client.

Important Perform maintenance on one ESXi host at a time. Avoid putting a host into maintenance mode if another host has not fully exited maintenance mode. If you need to do maintenance on more than one host in your on-premises environment, do one host at a time and complete the maintenance on one host and fully bring the host back out of maintenance mode before you initiate entering maintenance mode on the next host. If a host starts entering maintenance mode while another host has not fully exited maintenance mode, unexpected results might occur.

During ongoing system operations, the hosts have a number of running VMs, including:

- The Horizon Air Link.
- The management virtual appliance, which has a name in the pattern like *`smartnode-sm1`*. The specific name is unique to your system.
- VMs related to the desktop images and assigned desktops, including internal parent VMs that are created automatically by the VMware Instant Clone technology.

The hosts are in a vSAN cluster. When you initiate the task to put a host into maintenance mode, the VMware vSphere® vMotion™ capability starts migrating the host's running VMs to another host in the cluster. The management appliance detects that host is going into maintenance mode and automatically deletes the internal parent VMs from that host. When all of the VMs are evacuated from the host, it is in maintenance mode and you can perform your required maintenance tasks on it.

After you finish your maintenance tasks on the host, you take it out of maintenance mode. As new desktop provisioning occurs, the VMware Instant Clone technology creates parent VMs and instant clone VMs on the host as usual.

This procedure's steps are performed using the vSphere Web Client.

Note If you prefer to clear off all of the VMware Instant Clone technology's parent VMs on the host yourself before putting the host into maintenance mode, you can optionally perform the steps described in "Clear Internal Parent VMs off of a Horizon Cloud Node's ESXi Host," on page 88. If that is what you choose to do, you must perform those steps prior to initiating the enter-maintenance-mode process.

Prerequisites

Ensure the Horizon Cloud Node's management appliance is running before putting one of the hosts into maintenance mode. The management appliance handles the automatic deletion of parent VMs when one of the hosts enters maintenance mode. If the management appliance is not running when you select to put a host into maintenance mode, the enter maintenance mode task will fail.

Procedure

1 Use the vSphere Web Client to connect to your on-premises Horizon Cloud Node's vCenter Server environment.

2 Use the **VMs and Templates** view to verify the management appliance is powered on and running.

The management appliance has a name in the pattern like *`smartnode-sm1`*.

Important The management appliance must be running to ensure the parent VMs are automatically deleted successfully during this procedure.

3 Navigate to the ESXi host that you want to put into maintenance mode.

4 Put the host into maintenance mode by right-clicking the host and clicking **Maintenance Mode > Enter Maintenance Mode**.

- The management appliance detects the host is going into maintenance mode and automatically starts deleting the internal parent VMs.
- During the process of going into maintenance mode, the VMs residing on that host are automatically migrated from the host to other hosts in the cluster. End-user access to the desktops provided by those virtual machines remains unaffected.

5 Perform your maintenance tasks on the host as required.

6 Take the host out of maintenance mode by right-clicking the host and clicking **Maintenance Mode > Exit Maintenance Mode**.

As new provisioning occurs, the system creates parent VMs and instant clone VMs on the host as usual.

What to do next

If you cleared off the parent VMs yourself using the steps in "Clear Internal Parent VMs off of a Horizon Cloud Node's ESXi Host," on page 88, you should examine the `InstantClone.Maintenance` annotation value and make sure it is cleared out. If the value is 1 or 2, clear it out.

Clear Internal Parent VMs off of a Horizon Cloud Node 's ESXi Host

You might want to manually clear off the internal parent VMs that the VMware Instant Clone technology creates on an ESXi host prior to putting that host into maintenance mode.

These steps outline how to clear off the internal parent VMs using the vSphere Web Client with an on-premises system that has vSphere 6.5 or later.

Note If your system is built using vSphere 6.0.n, you cannot use the vSphere Web Client to perform these steps because the Custom Attributes widget which is not visible in the vSphere Web Client for versions 6.0.n. Instead, for vSphere 6.0.n systems, use the vSphere Client and in step 3, navigate to the host's Summary tab and its Annotations widget and click **Edit** to change the value of the `InstantClone.Maintenance` attribute.

Procedure

1 Use the vSphere Web Client to connect to your Horizon Cloud Node's vCenter Server 6.5.n environment.

2 Select the host.

3 Navigate to **Summary > Custom Attributes** and click **Edit**.

4 Set the `InstantClone.Maintenance` attribute's value to 1.

The system automatically starts deleting the parent VMs that are on the host. When the parent VMs on the host are deleted, the value for `InstantClone.Maintenance` changes to 2. During this time, the clones remain available for use but new clones are no longer created on the host.

The internal parent VMs are cleared off of that host.

Shut Down a Horizon Cloud Node

In certain situations, such as for site-wide power maintenance, you might need to shut down a Horizon Cloud Node completely, perform the maintenance or other operation, and power the node on again.

Shutting down a Horizon Cloud Node is rarely necessary. For example, you can perform maintenance on a Horizon Cloud Node by putting the hosts into maintenance mode one at a time. However, if necessary, you can achieve a complete shutdown by shutting down all the requisite virtual machines (VMs).

Note Because a vSAN cluster is part of the Horizon Cloud Node environment, information about shutting down a vSAN cluster is applicable to shutting down Horizon Cloud Nodes. See https://kb.vmware.com/kb/2142676 in preparation for the instructions that follow.

To completely shutdown the environment, perform the following steps on each Horizon Cloud Node in your deployed environment.

Prerequisites

- Enable access to the ESXi hosts used in your Horizon Cloud Node.

  ESXi access is required to shut down a Horizon Cloud Node. See VMware KB article 2004746 for more information about enabling ESXi access. Confirm that one of the following access methods is available.

Type of Access	Description
Direct Access	Enable the SSH service.
Remote Access	Use a remote-access technology, such as iLO or DRAC, to access the ESXi console.

- If your environment has active users, inform them of the shutdown and tell them to save and log out of their desktops to avoid data loss.
- Clear off the internal parent VMs from of all of the hosts by following the steps in "Clear Internal Parent VMs off of a Horizon Cloud Node's ESXi Host," on page 88. Clearing off the internal parent VMs before shutting down the system ensures that no unexpected results occur when the Horizon Cloud Node's management virtual appliance is powered off prior to putting the hosts into maintenance mode.

Procedure

1 Check for active user sessions to desktops or applications and if sessions exist, wait for them to end.

For example, click **Assign** to open the Assignments page to see the set of assignments. In turn, click each assignment to display its page, click **Desktops**, and check for active or disconnected sessions.

Caution Performing the shutdown while active or disconnected sessions are running causes unsaved user data to be lost.

2 Wait for active tasks running in the Horizon Cloud Node to end.

You can verify active tasks by connecting to the Horizon Cloud Node's vCenter Server Appliance using the vSphere Web Client. Do not proceed if vCenter Server tasks or vSAN resync processes are running.

a Wait for vCenter Server tasks, such as creating new desktop assignments or resizing existing assignments, to end.

b Wait for vSAN resync processes to end.

In the vSphere Web Client, you can view active resync processes by selecting the cluster and then navigating to **Monitor > Virtual SAN > Resyncing Components**.

3 Log into your vCenter Server Appliance using the vSphere Web Client.

4 Use the **VMs and Templates** view to access the folder that contains the desktops, such as the one labeled 1001.

5 Select all the desktop virtual machines in the folder and perform a shutdown.

6 Verify that you have completed the prerequisite step of clearing off the internal parent VMs from every host.

If you have not cleared off the internal parent VMs from all of the hosts, do it now.

7 Shut down the Horizon Air Link virtual machine and the Horizon Cloud Node management appliance in the following order.

- Horizon Air Link
- *smartnode-sm1*

8 Take note of the ESXi host on which the vCenter Server Appliance virtual machine is running and shut down any remaining virtual machines in the cluster as illustrated in the following list.

Note Your environment might not include all of the VMs listed below. For example, when a Horizon Cloud Node is built on a vSAN Ready Node, the environment does not have a VxRail Manager virtual machine.

- vRealize Log Insight
- VxRail Manager
- vCenter Server Appliance

9 Use an ESXCLI command to put each ESXi host in the cluster into maintenance mode, starting with the first host and continuing with the subsequent hosts.

You can access the hosts using the SSH client or by using a remote access technology, such as iLO or DRAC, to access the ESXi console.

```
esxcli system maintenanceMode set –e true –m noAction
```

10 Shut down each host in the cluster.

You can shut down the hosts using ESXCLI or PowerCLI commands or by connecting remotely using iLO or DRAC.

The following is an example of an ESXCLI command that shuts down a host, where *ReasonForShutdown* is a placeholder you can replace with the reason for the shutdown.

```
esxcli system shutdown poweroff –r "ReasonForShutdown"
```

What to do next

Perform the maintenance to the system or environment as required. After you perform the maintenance, power the Horizon Cloud Node on again. See "Power on the Horizon Cloud Nodes," on page 90.

Power on the Horizon Cloud Nodes

The procedure to power on Horizon Cloud Nodes requires you to use the same tools and technologies used to shut down the Horizon Cloud Nodes.

Note Because a vSAN cluster is part of the Horizon Cloud Node environment, information about shutting down a vSAN cluster is applicable to shutting down Horizon Cloud Nodes. See https://kb.vmware.com/kb/2142676 in preparation for the instructions that follow.

Perform the following steps on each Horizon Cloud Node in your environment.

Procedure

1 Power on each host in the cluster using a remote-access technology, such as iLO or DRAC.

2 Run an ESXCLI command to take each ESXi host in the cluster out of maintenance mode, starting with the first host and continuing with the subsequent hosts.

You can access the hosts using the SSH client or by using a remote access technology, such as iLO or DRAC, to access the ESXi console.

```
esxcli system maintenanceMode set –e false
```

3 Using the vSphere Host Client, access the ESXi host on which the vCenter Server Appliance virtual machine (VM) is located and power on the VM.

After several minutes, the vCenter Server Appliance VM powers on.

4 Reconnect to the vCenter Server Appliance using the vSphere Web Client.

5 Starting with the first ESXi host and continuing with each host in the cluster, navigate to **Summary > Custom Attributes**, click **Edit**, and verify the `InstantClone.Maintenance` attribute has no value set.

If the `InstantClone.Maintenance` attribute has a value set, clear out the value.

Note If your cluster uses vSphere 6.0.n, you cannot perform this step using the vSphere Web Client. Instead, use the vSphere Client to navigate to each hosts's **Summary > Annotations** to edit the `InstantClone.Maintenance` attribute.

6 If the following virtual machines are located on hosts in the cluster, power them on in the order listed below.

Note Your environment might not include all of the VMs listed below. For example, when a Horizon Cloud Node is built on a vSAN Ready Node, the environment does not have a VxRail Manager virtual machine.

- VxRail Manager
- vRealize Log Insight

7 Power on the *smartnode*–sm1 appliance and the Horizon Air Link virtual machine in the following order.

- *smartnode*-sm1
- Horizon Air Link

8 In the Administration Console, navigate to the desktop assignments and power on the desktops within each assignment.

a Log in to Horizon Cloud at https://cloud.horizon.vmware.com.

b Click **Assign**.

c Click the name of a desktop assignment.

d Click **Desktops**.

e Select the check boxes next to each desktop that you want to power on.

f Select **... > Power On**.

g Repeat steps Step 8c through Step 8f for each desktop assignment.

What to do next

Continue using your environment to confirm the system functions as normal.

Updating Horizon Cloud with On-Premises Infrastructure

VMware updates the Horizon Cloud with On-Premises Infrastructure software components periodically to include new features and bug fixes. VMware typically updates the in-cloud management environment on a weekly basis and updates the Horizon Cloud Node software components on a roughly quarterly basis. The normal update process takes place without incurring any system downtime.

An update affects the following components.

- Horizon Cloud environment, running in the cloud.
- On-premises Horizon Cloud Node software, running in a hyper-converged appliance, such as VxRail or vSAN Ready Node.
- VMware agents used in the master images

On-Premises Horizon Cloud Node Software Updates

The Horizon Cloud Node software update process is performed in the following stages.

1 Downloading new software, an automatic process

2 Scheduling the update

3 Migrating to the new version

The first stage, downloading new software, takes place when a new version of software is available. Horizon Cloud triggers the Horizon Air Link appliance to download the new version of the software. The Horizon Air Link appliance builds an inactive parallel environment. This stage is transparent to you and does not cause any downtime.

When the first stage finishes, the Administration Console signifies that an update is available.

To check the update availability for a Horizon Cloud Node, select **Settings > Infrastructure** and click a node. If an update is available, an on-screen message describing the update appears next to the software version number.

The second stage, scheduling the update, occurs between you and the VMware Operations team. Arrange a convenient time for the update to take place. Typically, the update itself, or the migration from the existing version to the new version, takes about five minutes. As a best practice, schedule the update at a time when the environment is least busy. After the update is scheduled, the Administration Console displays the scheduled time in a top banner. To reschedule the update, contact VMware Operations.

The third stage, migration to the new version, takes place at the scheduled time, at which point, VMware Operations trigger the migration. The process takes around five minutes to complete, and migrates the data and configuration from the running environment to the new environment. During the migration, the following rules apply.

- You cannot perform administrative tasks or log in to the Administration Console.
- Any end users attempting to connect to desktops cannot do so.
- End users with connected desktop sessions can continue to use their systems without any downtime.

When the update finishes, you can log back in to the Administration Console. To see the software version currently running, select **Settings > Infrastructure** and click a node. The page displays the current software version running. Click the software version number to see associated release information.

You can now update the guest operating system agents.

Note After a Horizon Cloud Node update, the old environment remains in the system in a powered-off state in case rollback is needed. The old powered-off environment is automatically deleted after 30 days.

Update the VMware Agents

When the update of the Horizon Cloud Node is complete, you can update the respective VMware agents in your master desktop virtual machines to finish the update process.

Prerequisites

- Verify that your Horizon Cloud Node system is updated. See "Updating Horizon Cloud with On-Premises Infrastructure," on page 91.
- Download the new agents from the My VMware site.

Procedure

1. In the Administration Console, select **Inventory > Images**, select the check box next to the image to update, and click **Duplicate**.
2. Provide a name for the new image and click **Save**.
3. On the Images page, refresh the page until the status of the image you duplicated changes to Published, which might take a few minutes, click **New**, and enter the name you provided for the duplicate image in the **Desktop** text box.

   A dialog box appears prompting you to power on the desktop.

4 Click **Power On**.

The New Image dialog box appears and values refresh in the box as the desktop's associated virtual machine powers on.

5 Click the IP address to access the desktop using a remote desktop connection

The system downloads a Remote Desktop Protocol (RDP) file so you can access the desktop using the RDP client. If a dialog box does not automatically appear for creating a remote desktop connection to the desktop, locate the downloaded `RichClient.rdp` and click it.

6 In the remote desktop connection window, click the button to accept the connection.

7 Log in to the desktop operating system and update it as required for your organization's needs, including installing the updated agents.

8 In the Administration Console's New Image dialog box, update any additional required information until the **Publish** button is available.

Scroll through the New Image dialog box to verify all the required text boxes are filled in.

9 Click **Publish**.

The image publishes.

10 On the Images page, refresh the page until the status of the image you duplicated changes to Published, which might take a few minutes

11 Select the check box next to the image, click **...**, and select **Push Updates**.

The Push Updates dialog box appears.

12 Select the check box next to the assignments to update and click **OK**.

The updated master desktop VM containing the updated agents replaces the desktop VMs in the assignments you selected.

The next time users log in, they each receive an updated image.

11 Access Desktops and Applications

After you create desktop and application assignments, end users can access desktops and applications using the Horizon Client or a browser if HTML access is configured. If you have integrated your environment with your VMware Identity Manager environment, you can optionally enforce end-user access to go through the Workspace ONE portal.

This chapter includes the following topics:

Log in to the Desktop Using the Horizon Client

When your end users log in and launch their desktops, they can start running the applications and performing tasks such as accessing USB and other devices connected to their local computers, sending documents to any printers that the local computer can detect, and using multiple display monitors.

These steps describe using a VMware Horizon Client for the first time to launch a desktop provided by your Horizon Cloud with On-Premises Infrastructure environment.

Prerequisites

- Familiarize yourself with the most up-to-date information regarding VMware Horizon Clients. For example, to check for up-to-date VMware Horizon Client support information, see the VMware Product Interoperability Matrixes at https://www.vmware.com/resources/compatibility/sim/interop_matrix.php and to see the respective documentation, see the VMware Horizon Clients documentation page at https://www.vmware.com/support/viewclients/doc/viewclients_pubs.html.
- From your organization's DNS information, obtain the fully qualified domain name that is associated with the IP address that this Horizon Cloud Node uses for desktops, such as `desktops.mycorp.com`. See the steps in "Determine the Horizon Cloud Node IP Address for Use by Desktops," on page 81 for how to use the Administration Console to view the IP address that is assigned to this Horizon Cloud Node.

Procedure

1. Start the VMware Horizon Client.
2. If you did not configure a certificate for your environment, accept the untrusted connection.
3. Select the choices in the VMware Horizon Client for adding a new server.
4. In the new server configuration, enter the name that was added to the DNS for the environment, for example, `desktops.mycorp.com`.
5. Enter the credentials for your Active Directory user in the authentication dialog box.

6 If two-factor authentication is configured, enter RSA or RADIUS credentials.

7 Select the desktop that you want to launch from the displayed list.

8 (Optional) For advanced configuration, right-click the desktop and make your selection.

Log in to the Desktop Using a Browser

If your Horizon Cloud with On-Premises Infrastructure environment is configured for HTML Access, users can access desktops and applications by pointing their browser to the fully qualified domain name that your organization has associated with the Horizon Cloud Node IP address.

These steps describe using a browser to launch a desktop provided by your Horizon Cloud with On-Premises Infrastructure environment.

Note If integration with a VMware Identity Manager environment is configured and the User Account Configuration settings in the General Settings page are set to **Yes**, instead of this procedure, end users must access their desktops from Workspace ONE portal. See "Enforce End-User Access Through VMware Identity Manager," on page 96.

Prerequisites

From your organization's DNS information, obtain the fully qualified domain name that is associated with the IP address that this Horizon Cloud Node uses for desktops, such as `desktops.mycorp.com`. See the steps in "Determine the Horizon Cloud Node IP Address for Use by Desktops," on page 81 for how to use the Administration Console to view the IP address that is assigned to this Horizon Cloud Node.

Note In previous releases, this IP address was called the tenant appliance IP. The Horizon Cloud Node virtual appliance has two IP addresses: one on the management network and one on the desktop network. Obtain the FQDN that is associated with the Horizon Cloud Node IP address that is from the desktop network.

Verify that you have the credentials for a user that has a desktop assignment.

Procedure

1 Point a browser to a URL of the form `https://<Node-FQDN>`, where *Node-FQDN* is the fully qualified domain name that your organization has associated with the IP address for this Horizon Cloud Node.

For example, if your company's DNS associates the node IP address with an FQDN of `myDesktops.example.com`, point the browser to `https://myDesktops.example.com`.

2 Sign in using the credentials for a user that has a desktop assignment.

Icons representing the user's assignments are displayed in the browser. The user can launch a desktop or application by clicking its icon.

Enforce End-User Access Through VMware Identity Manager

When your Horizon Cloud Node environment is integrated with your VMware Identity Manager environment, you can specify that end users must use the Workspace ONE portal to access their desktops. Requiring end users to access their desktops through the Workspace ONE portal prevents direct desktop access using their Horizon Client or by HTML access. This enforcement is useful when you want to use the two-factor authentication method that is set in your VMware Identity Manager environment.

Your end users typically launch their entitled desktops using the following methods.

- From a browser, by loading the FQDN associated with your Horizon Cloud Node.
- From the Horizon Client application, by including your Horizon Cloud Node FQDN as a new server location in the client application.

- From the Workspace ONE portal, if your environments are integrated.

You can optionally configure your Horizon Cloud Node environment to require using the Workspace ONE portal only.

You can configure enforcement on users who are accessing their desktops from locations outside your corporate network or on users accessing from inside your corporate network, or both. When using the Workspace ONE portal is enforced, users that try to access their desktops other than from the Workspace ONE portal see a message informing them to use the portal.

Prerequisites

Verify that your environments are integrated, by completing the steps described in Chapter 8, "Integrate Horizon Cloud with On-Premises Infrastructure with a VMware Identity Manager Environment," on page 67.

Procedure

1 In the Administration Console, navigate to **Settings > General Settings** and click **Edit**.

2 In the User Account Configuration section, make selections according to your organization's needs.

Option	Description
Force Remote Users to vIDM	When set to **Yes**, users that are trying to access their desktops from locations outside of your corporate network must log in to their Workspace ONE portal and access desktops from that portal.
Force Internal Users to vIDM	When set to **Yes**, users that are trying to access their desktops from locations within your corporate network must log in to their Workspace ONE portal and access desktops from that portal.

3 Click **Save** to confirm the configuration to the system.

What to do next

Verify that the desktop access behaves according to your settings by trying to access a desktop using the Horizon Client or using a browser directly instead of from the Workspace ONE portal.

Index

V

W