Horizon Upgrades

VMware Horizon 2111

vmware®

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

https://docs.vmware.com/

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

Contents

VMware Horizon Upgrades to this Version

Horizon Upgrades provides instructions for upgrading from the latest main or maintenance releases of VMware Horizon™ 7.x and VMware Horizon 2xxx to this version. You can also use this guide when you upgrade to VMware Horizon maintenance releases.

If you are also upgrading your version of VMware vSphere®, this guide tells you which steps of that upgrade to do at various stages of the VMware Horizon upgrade.

Intended Audience

This guide is intended for anyone who needs to upgrade to this latest version of this product. The information in this guide is written for experienced Microsoft Windows or Linux system administrators who are familiar with virtual machine technology and datacenter operations.

VMware Horizon Upgrade Overview

1

Upgrading an enterprise VMware Horizon deployment involves several high-level tasks. Upgrading is a multistage process in which procedures must be performed in a particular order.

Attention For supported upgrade paths, see the VMware Product Interoperability Matrix.

You must complete the upgrade process in a specific order. Order is also important within each upgrade stage.

Note This overview relates to upgrades for major, minor, and maintenance releases.

How many of the following tasks you need to complete depends on which components of VMware Horizon you use in your deployment.

1. If you have features that are no longer supported in the latest version of VMware Horizon, you must uninstall some of these features before proceeding with the upgrade. See Chapter 2 Uninstalling No Longer Supported and Deprecated Features.
2. Upgrade the Horizon Client software that runs on end users' client devices. See Chapter 3 Upgrade the Client Application.
3. On the physical or virtual machines that host Connection Server instances, make backups and record various configuration and system settings. See Preparing Connection Server for an Upgrade.

   If you have multiple Connection Server instances in a replicated group, make backups and record configuration settings for only one instance in the group. For other preparation tasks, you can perform the tasks for one instance at a time, just before you perform the upgrade of that server instance.
4. Upgrade Connection Server instances. See Upgrade Connection Servers in a Replicated Group.

   In a typical production environment that consists of two or more Connection Server instances fronted by a load balancer, you need to remove Connection Server instances from the load balanced cluster while they are upgraded.

   Important After you upgrade a Connection Server instance to the latest version, you cannot downgrade that instance to an earlier version. After you upgrade all Connection Server instances in a replicated group, you cannot add another instance that runs an earlier version.

5 Upgrade the group policies used in Active Directory. See Using Horizon Group Policy Administrative Template Files.

6 If you are also upgrading VMware vSphere components, upgrade vCenter Server. See Upgrade vCenter Server.

   During the vCenter Server upgrade, existing remote desktop and application sessions will not be disconnected. Remote desktops that are in a provisioning state will not get powered on during the vCenter Server upgrade, and new desktops cannot be launched during the vCenter Server upgrade.

7 If you are also upgrading vSphere, upgrade the VMware® ESXi™ hosts and virtual machines. See Chapter 6 Upgrade ESXi Hosts and Their Virtual Machines.

   ESXi hosts can be upgraded with zero down time by vMotioning the virtual machines to another host in the cluster, if hosts are configured under clustered environment.

8 If you currently use Windows Terminal Services servers as desktop sources, upgrade to Windows Server 2012 R2 or later and verify that the RDS Host role is installed. See Upgrade RDS Hosts That Provide Session-Based Desktops

9 Upgrade the Horizon™ Agent software that runs on the physical or virtual machines that are used as templates for desktop cloning, as full-clone desktops in a pool, and as individual desktops in a manual pool. See Upgrade Horizon Agent.

10 Use the newly upgraded virtual machine desktop sources to create upgraded pools of desktops. See Upgrade Instant-Clone Desktop Pools When You Upgrade vCenter Server to vSphere 6.7 or Later.

11 If you use the Cloud Pod Architecture feature, see Upgrading a Cloud Pod Architecture Environment.

Because certain commands can simultaneously upgrade more than one stage, VMware recommends that you thoroughly understand the irreversible changes at each stage before you upgrade your production environments.

Deploying an Extended Service Branch

Approximately once a year, VMware designates one VMware Horizon release as an Extended Service Branch (ESB). An ESB is a parallel release branch to the existing Current Releases (CR) of the product. By choosing to deploy an ESB, customers receive periodic service packs (SP) updates, which include cumulative critical bug fixes and security fixes. Most importantly, there are no new features in the SP updates, so customers can rely on a stable Horizon platform for their critical deployments.

For more information on the ESB and the Horizon versions that have been designated an ESB, see VMware Knowledge Base article 86477.

Uninstalling No Longer Supported and Deprecated Features

2

Before you upgrade VMware Horizon, you must uninstall features that are no longer supported or deprecated in the latest version of VMware Horizon.

If you upgrade to VMware Horizon 2012 and later, you must uninstall the following features that are available in earlier releases of VMware Horizon 7.x:

No Longer Supported or Deprecated Features	Description
Security Server (no longer supported)	If you have security servers and want to upgrade to VMware Horizon 2012 and later, you must deploy a replacement Unified Access Gateway appliance and then uninstall the security servers before upgrading Connection Server. **Note** After an upgrade to VMware Horizon 2012 if you don't remove the security server and try to connect to Horizon Client using the security server, you get an HTTP error. See Replacing a Security Server with a Unified Access Gateway Appliance.
JMP Server (no longer supported)	If you have a JMP Server installed, and want to upgrade to VMware Horizon 2012 and later, you must uninstall the JMP server. See Uninstall JMP Server. **Note** Previously created JMP desktop assignments still appear in Horizon Console and can be modified or deleted. Previously created App Volumes assignments created from JMP assignments still appear in the App Volumes console and can be modified or deleted. The Dynamic Environment Manager setting assignment created from the JMP assignment if the Dynamic Environment Manager share isn't removed during JMP uninstallation, appears in the read only mode in the Dynamic Environment Manager console and you cannot modify or delete this assignment.
View Composer (no longer supported)	If you have View Composer installed, and want to upgrade to VMware Horizon 2012 and later, you must remove View Composer and delete all your linked-clone desktop pools and farms. See Remove View Composer from Horizon.

This chapter includes the following topics:

- Uninstall JMP Server
- Remove View Composer from Horizon

Replacing a Security Server with a Unified Access Gateway Appliance

Replace a security server with a Unified Access Gateway appliance.

Procedure

1. Uninstall the security server software.
2. Remove the security server's LDAP entry: `vdmadmin -S [-b` *authentication_arguments*`] -r -s` *server*

   See *Removing the Entry for a Connection Server Instance Using the -S Option* in the *Horizon Administration* document.
3. In Horizon Console, register the Unified Access Gateway appliance.
4. At the network firewall between Unified Access Gateway and Connection Server, remove firewall rules associated with the removed security server and add firewall rules associated with the incoming Unified Access Gateway. The Unified Access Gateway needs to communicate with Connection Server on TCP port 443.

   The back-end firewall rules for Security Server to Connection Server are as follows:

Source	Default Port	Protocol	Destination	Default Port	Notes
Security Server	UDP 500	ISAKMP	Connection Server	UDP 500	IPsec phase 1 negotiation.
Security Server	UDP 4500	NAT-T	Connection Server	UDP 4500	Encapsulated AJP13 traffic when using NAT.
Security Server		ESP	Connection Server		Encapsulated AJP13 traffic when NAT traversal is not required. ESP is IP protocol 50. Port numbers are not specified.
Security Server		AJP13	Connection Server	TCP 8009	AJP13 traffic without IPsec and during pairing.
Security Server		JMS	Connection Server	TCP 4001	Message channel for key negotiation.
Security Server		JMS-TLS	Connection Server	TCP 4002	Message channel for management.

5. Configure and start the Unified Access Gateway appliance.

   See *Deploying and Configuring VMware Unified Access Gateway* document in https://docs.vmware.com/en/Unified-Access-Gateway/index.html.

Uninstall JMP Server

If you have a JMP Server installed, and want to upgrade to VMware Horizon 2006 and later, you must uninstall the JMP server before proceeding with the upgrade.

Prerequisites

- Verify that you have the correct administrative privileges to uninstall JMP Server.

Procedure

1. Complete the following steps to delete Dynamic Environment Manager configuration share information for the JMP Server.
   a. In Horizon Console, click **JMP Configuration**.
   b. Click the **UEM** tab.
   c. Select the row for the Dynamic Environment Manager configuration share information that you want to delete from JMP Settings.
   d. Click **Delete** to confirm that you do want to delete this Dynamic Environment Manager configuration share information.

   If there are no JMP assignments that use the Dynamic Environment Manager configuration share, it is removed.

   If the Dynamic Environment Manager configuration share is in use by any JMP assignment, a warning dialog box appears. The warning message includes the list of JMP assignments that are using the Dynamic Environment Manager configuration share. You can delete the Dynamic Environment Manager configuration share information only after you remove it from the JMP assignments or delete those JMP assignments that use it.
2. Complete these steps to uninstall JMP Server.
   a. Open the Microsoft Windows Program and Features console.

      For example, click **Start > Settings > System > Apps and Features**.
   b. Select **VMware JMP** from the list of installed applications.
   c. To finish the uninstallation steps, click **Uninstall** and follow the wizard.

Remove View Composer from Horizon

You can remove the connection between Horizon and the View Composer service that is associated with a vCenter Server instance.

Before you disable the connection to View Composer, you must remove from Horizon all the linked-clone virtual machines created by View Composer. Horizon prevents you from removing View Composer if any associated linked clones still exist. After the connection to View Composer is disabled, Horizon cannot provision or manage new linked clones.

Procedure

1 Remove the linked-clone desktop pools created by View Composer.

   a In Horizon Console, select **Inventory > Desktops**.

   b Select a linked-clone desktop pool and click **Delete**.

      A dialog box warns that you will permanently delete the linked-clone desktop pool from Horizon. If the linked-clone virtual machines are configured with persistent disks, you can detach or delete the persistent disks.

   c Click **OK**.

      The virtual machines are deleted from vCenter Server. In addition, the associated View Composer database entries and the replicas created by View Composer are removed.

   d Repeat these steps for each linked-clone desktop pool created by View Composer.

2 Navigate to **Settings > Servers**.

3 On the **vCenter Servers** tab, select the vCenter Server instance with which View Composer is associated.

4 Click **Edit**.

5 On the **View Composer** tab, under **View Composer Server Settings**, select **Do not use View Composer**, and click **OK**.

Results

You can no longer create linked-clone desktop pools in this vCenter Server instance, but you can continue to create and manage full virtual-machine desktop pools in the vCenter Server instance.

Upgrade the Client Application

3

Upgrade to the latest version of Horizon Client and upgrade the firmware on thin client devices if you use them.

Important Upgrading involves running the new version of the Horizon Client installer without first removing the older version of the client application. If your end users have the Windows-based Horizon Client 4.6.0 or an earlier version, instruct them to remove the client software before downloading and running the latest Horizon Client installer.

Prerequisites

- Verify that you have a domain user account with administrative privileges on the hosts that you will use to run the installer and perform the upgrade.
- Verify that the client desktop, laptop, tablet, or phone meets the operating system requirements and hardware requirements of Horizon Client. See the "Using Horizon Client" document for the specific type of desktop or mobile client device. Go to https://docs.vmware.com/en/VMware-Horizon-Client/index.html.

Procedure

1 Have end users upgrade to the latest version of Horizon Client.

Option	Action
Horizon Client	Download and send the Horizon Client installers to your end users or post them on a Web site and ask end users to download the installer and run it. You can download the installers or have your end users download them from the VMware Web site at https://www.vmware.com/go/viewclients. For mobile clients, you can alternatively instruct your end users to get the latest version of Horizon Client from other Web sites that sell apps, including the Apple App Store, Google Play, Amazon, and Windows Store.
VMware Horizon user Web portal	End users can open a browser and browse to a Connection Server instance. The Web page that appears is called the VMware Horizon user Web portal, and it contains links for downloading the installer file for Horizon Client. **Note** The default links in Web page point to the Horizon Client download site. You can change the default links to point elsewhere. See "Configure the VMware Horizon Web Portal Page for End Users" in the *Horizon Installation* document.
Thin client	Upgrade the thin client firmware and install the new Horizon Client software on end users' client devices. Thin clients and zero clients are provided by VMware partners.

2 Have end users verify that they can log in and connect to their remote desktops.

System Requirements for VMware Horizon Server Upgrades

4

Hosts and virtual machines in a VMware Horizon deployment must meet specific hardware and operating system requirements.

This chapter includes the following topics:

Compatibility Matrix for Various Versions of VMware Horizon Components

Because large enterprises must often perform phased upgrades, components are designed to be somewhat forward and backward compatible during upgrades.

The following versions are supported for upgrading to VMware Horizon :

- VMware Horizon 7 version 7.x

To determine the latest maintenance release of a particular component, see the Release Notes for that release, available from https://docs.vmware.com/en/VMware-Horizon-7/index.html

Horizon Connection Server compatibility with Horizon Agents is limited to interoperability during a Connection Server upgrade. You must upgrade Horizon Agents as soon as possible to match the version of the Connection Server that manages them.

The following table lists the components and show whether they are compatible with other components whose version is different.

Table 4-1. Compatibility Matrix for VMware Horizon 2006 or Later and Earlier Versions of VMware Horizon Components

	Connection Server: Earlier Version	Horizon Agent: Earlier Version	Horizon Client (Windows): Earlier Version
Connection Server 2006 or later	Only during upgrade	Only during upgrade	No
Horizon Agent 2006 or later	Only during upgrade	N/A	Only during upgrade
Horizon Client 2006 or later	Yes	Yes	N/A

For details about which versions of Horizon are compatible with which versions of vCenter Server and ESXi, see the VMware Product Interoperability Matrix at http://www.vmware.com/resources/compatibility/sim/interop_matrix.php.

Horizon Connection Server Requirements

Horizon Connection Server acts as a broker for client connections by authenticating and then directing incoming user requests to the appropriate remote desktops and applications. Horizon Connection Server has specific hardware, operating system, installation, and supporting software requirements.

Hardware Requirements for Horizon Connection Server

You must install all Horizon Connection Server installation types, including standard, replica, and enrollment server installations, on a dedicated physical or virtual machine that meets specific hardware requirements.

Table 4-2. Horizon Connection Server Hardware Requirements

Hardware Component	Required	Recommended
Processor	Pentium IV 2.0GHz processor or higher	4 CPUs
Network Adapter	100Mbps NIC	1Gbps NICs
Memory	4GB RAM or higher	At least 10GB RAM for deployments of 50 or more remote desktops

These requirements also apply to replica Horizon Connection Server instances that you install for high availability or external access.

Important The physical or virtual machine that hosts Horizon Connection Server must have an IP address that does not change. In an IPv4 environment, configure a static IP address. In an IPv6 environment, machines automatically get IP addresses that do not change.

Supported Operating Systems for Horizon Connection Server

You must install Horizon Connection Server on a supported Windows Server operating system.

For a list of supported Windows Server operating systems, see the VMware Knowledge Base (KB) article https://kb.vmware.com/s/article/78652.

Upgrade Requirements for Horizon Connection Server

The Horizon Connection Server upgrade process has specific requirements and limitations.

- Connection Server requires a valid license for this latest release. If you have a perpetual license, you will need to download the new key specific for VMware Horizon 2006 or later releases. If you have a subscription license, no additional action is required.
- The domain user account that you use to install the new version of Connection Server must have administrative privileges on the Connection Server host. The Connection Server administrator must have administrative credentials for vCenter Server.
- When you run the installer, you authorize an Administrators account. You can specify the local Administrators group or a domain user or group account. VMware Horizon assigns full Horizon Administration rights, including the right to install replicated Connection Server instances, to this account only. If you specify a domain user or group, you must create the account in Active Directory before you run the installer.
- When you back up Connection Server, the Horizon Directory configuration is exported as encrypted LDIF data. To restore the encrypted backup VMware Horizon configuration, you must provide the data recovery password. The password must contain between 1 and 128 characters.

Security-Related Requirements

- Connection Server requires a TLS certificate that is signed by a CA (certificate authority) and that your clients can validate. Although a default self-signed certificate is generated in the absence of a CA-signed certificate when you install Connection Server, you must replace the default self-signed certificate as soon as possible. Self-signed certificates are shown as invalid in Horizon Console.

  Also, updated clients expect information about the server's certificate to be communicated as part of the TLS handshake between client and server. Often updated clients do not trust self-signed certificates.

  For complete information about security certificate requirements, see "Configuring TLS Certificates for Horizon Servers" in the *Horizon Installation* guide. Also see the *Scenarios for Setting Up TLS Certificates for Horizon* document, which describes setting up intermediate servers that perform tasks such as load balancing and off-loading SSL connections.

  Note If your original servers already have TLS certificates signed by a CA, during the upgrade, VMware Horizon imports your existing CA-signed certificate into the Windows Server certificate store.

- Certificates for vCenter Server and VMware Horizon servers must include certificate revocation lists (CRLs). For more information, see "Configuring Certificate Revocation Checking on Server Certificates" in the *Horizon Installation* document.

  Important If your company uses proxy settings for Internet access, you might have to configure your Connection Server hosts to use the proxy. This step ensures that servers can access certificate revocation checking sites on the Internet. You can use Microsoft Netshell commands to import the proxy settings to Connection Server. For more information, see "Troubleshooting Horizon Server Certificate Revocation Checking" in the *Horizon Installation* document.

- You might need to make security protocol configuration changes to continue to be compatible with vSphere. If possible, apply patches to ESXi and vCenter Server to support TLSv1.1 and TLSv1.2 before upgrading Connection Server.

If you plan to perform fresh installations of Connection Server instances on additional physical or virtual machines, see the complete list of installation requirements in the *Horizon Installation* document.

Requirements and Considerations for Horizon Agent

The Horizon Agent component assists with session management, single sign-on, device redirection, and other features. You must install Horizon Agent on all virtual machines, physical systems, and RDS hosts.

The types and editions of the supported guest operating system depend on the Windows version.

For a list of Windows 10 guest operating systems, see the VMware Knowledge Base (KB) article https://kb.vmware.com/s/article/78714.

For Windows operating systems, other than Windows 10, see the VMware Knowledge Base (KB) article https://kb.vmware.com/s/article/78715.

For enhanced security, VMware recommends configuring cipher suites to remove known vulnerabilities. For instructions on how to set up a domain policy on cipher suites for Windows machines that run Horizon Agent, see the topic about disabling weak ciphers for Horizon Agent in the *Horizon Installation* document.

Upgrading VMware Horizon Server Components

5

The server components that you must upgrade include Horizon Connection Server and replicated servers.

If you spread the upgrade tasks across multiple maintenance windows, you can verify success or discover issues at each phase of the process. VMware recommends upgrading all server components during the first maintenance window.

This chapter includes the following topics:

Upgrading Horizon Connection Server

If your deployment uses load balancers to manage multiple Connection Server instances, an upgrade of the Connection Server infrastructure can be performed with zero down time.

After you have performed a fresh install or upgraded all Connection Server instances to VMware Horizon 2006, you cannot downgrade the Connection Server instances to a version earlier than Horizon 7 version 7.2 because the keys used to protect LDAP data have changed.

To keep the possibility of downgrading Connection Server instances while planning an upgrade to VMware Horizon 2006, you must backup the Connection Server instances before starting the upgrade. If you need to downgrade the Connection Server instances, you must downgrade all Connection Server instances and then apply the backup to the last Connection Server that is downgraded.

When upgrading from a version of VMware Horizon earlier than Horizon 7 version 7.8, some user authentication settings will change. How these user authentication settings affect the user experience depends upon the client. See the Horizon Client documentation at https://docs.vmware.com/en/VMware-Horizon-Client/index.html. You must understand the usability and security implications of the user authentication settings before changing them. See, "Security-Related Server Settings for User Authentication" in the *Horizon Security* document.

If you have a perpetual license, after upgrading a Connection Server in a pod to VMware Horizon 2006, you cannot start a desktop from this Connection Server but you can start a desktop from other Connection Servers in the pod. To start a desktop from the upgraded Connection Server, start Horizon Console on this Connection Server and enter a 2006 license key. Then, you can start desktops from all Connection Servers in the pod.

After upgrading a Connection Server instance, perform a hard reload of the Horizon Console browser, so that it picks the latest HTML5 UI source code from the Connection Server.

Preparing Connection Server for an Upgrade

Before you upgrade Connection Server or before you upgrade any of the vSphere components that Connection Server relies on, you must perform several tasks to ensure that these upgrades are successful.

Tasks to Perform on Only One Instance in a Replicated Group

Before you begin upgrading any Connection Server instances, perform the following tasks using only one of the instances. Because the instances are replicated, the settings on one instance are the same as the settings on the others:

- If Connection Server is installed in a virtual machine, take a snapshot of the virtual machine.

  For instructions on taking snapshots, see the vSphere Client online help. If you ever need to revert to this snapshot and if you have other Connection Server instances in a replicated group, you must uninstall those instances before you revert the golden image to the snapshot. After you revert, you can reinstall the replicated instances and point to the instance you reverted.

  You can label the snapshot Upgrade Preparation Phase.

- Open Horizon Console and document all the global settings and settings for desktops and pools.

  You can also take a screen shot of the applicable settings.

- Use the `vdmexport.exe` utility to back up the Horizon LDAP.

  For instructions, see the administration guide for your current version of the *Horizon Administration* document.

Tasks to Perform for Each Instance Just Before Upgrading

- Verify that the virtual or physical machine on which the current Connection Server instance is installed meets the system requirements for the new version.

See Horizon Connection Server Requirements.

- Document the IP address and system name of the machine on which Connection Server is installed.
- Determine if your company has written any batch files or scripts that run against the Horizon LDAP database on the Connection Server instance, and if so, document their names and locations.
- Open Horizon Console and document all the settings that are specific to this instance.

  For example, go to **Settings > Servers > Connection Servers**, select the Connection Server instance in the table and click **Edit**. You can take a screen shot of each tab in the **Edit Connection Server Settings** dialog box.

Upgrade Connection Servers in a Replicated Group

This procedure describes upgrading Connection Server instances. For example, this procedure applies to Connection Servers that are configured for connections to clients that are inside the corporate firewall.

You do not need to reboot the Connection Server after the upgrade completes.

Note This procedure describes an in-place upgrade. To migrate to a different machine, see Upgrade to the Latest Version of Connection Server on a Different Machine.

Prerequisites

- Determine when to perform this procedure. Choose an available desktop maintenance window. The amount of time the upgrade takes depends on the number of Connection Server instances in the group. Budget 15 minutes to half an hour for each instance.
- Familiarize yourself with the security-related requirements of VMware Horizon, and verify that these requirements are met. See Upgrade Requirements for Horizon Connection Server. You might need to obtain and install a CA-signed SSL server certificate that includes certificate revocation information, verify that Windows Firewall with Advanced Security is set to **on**, and configure any back-end firewalls to support IPsec.
- Verify that the server on which vCenter Server is installed has a CA (certificate authority)-signed SSL server certificate installed and configured. After you upgrade Connection Server, if vCenter Server does not use a CA-signed certificate, the default self-signed certificate is shown as invalid in Horizon Console, and a message indicates that vCenter Server is unavailable.
- Complete the tasks listed in Preparing Connection Server for an Upgrade.
- Verify that you have a license that is valid for the new version.
- Verify that you have a domain user account with administrative privileges on the hosts that you use to run the installer and perform the upgrade.

- If you are unfamiliar with the `vdmexport.exe` utility, print the instructions for using it from the *Horizon Administration* document. You will use this utility to back up the Horizon LDAP database as part of the upgrade procedure.

You do not need to make any changes to the configuration of existing load balancers.

Procedure

1. If you are using a load balancer to manage a group of Connection Server instances, disable the server that hosts the Connection Server instance that you are about to upgrade.
   a. Log in to Horizon Console.
   b. Go to **Settings > Servers** and click the **Connection Servers** tab.
   c. Select the Connection Server instance in the list and click the **Disable** button above the table.
   d. To confirm disabling the server, click **OK**.
2. On the host of the Connection Server instance, download and run the installer for the new version of Connection Server.

   The installer filename is `VMware-Horizon-Connection-Server-x86_64-y.y.y-xxxxxx.exe`, where *xxxxxx* is the build number and *y.y.y* is the version number. You do not need to stop any services before performing the upgrade. The installer stops and restarts services as necessary. In fact, the VMwareVDMDS service must be running to upgrade the Horizon LDAP database.

   The installer determines that an older version is already installed and performs an upgrade. The installer displays fewer installation options than during a fresh installation.

   The Horizon LDAP database is also upgraded.

   Note Before performing the upgrade, the installer determines whether the server can communicate with the other servers in the replicated group and whether the server can fetch LDAP updates from the other servers in the group. If the status check fails, the upgrade does not proceed.
3. Verify that the VMware Horizon Connection Server service restarts after the installer wizard closes.
4. Log in to VMware Horizon and enable the Connection Server instance that you just upgraded.
   a. Go to **Settings > Servers** and click the **Connection Servers** tab.
   b. Select the Connection Server instance in the list and click the **Enable** button above the table.
   c. In the Version column, verify that the new version is displayed.
5. Go to **Settings > Product Licensing and Usage**, click **Edit License**, enter the license key, and click **OK**.

6 If you are using a load balancer for managing this Connection Server instance, enable the server that you just upgraded.

7 Verify that you can log in to a remote desktop.

8 To upgrade each Connection Server instance in the group, repeat the previous steps.

Important If you do not upgrade all Connection Server instances in a replicated group, the health indicators in the Horizon Console dashboard might show that one or more instances are in an error state. This situation arises because different versions supply different kinds of data. The solution is to upgrade all instances in the replicated group.

9 Use the `vdmexport.exe` utility to back up the newly upgraded Horizon LDAP database.

If you have multiple instances of Connection Server in a replicated group, you need only export the data from one instance.

10 Log in to and examine the Horizon Console to verify that the vCenter Server icon is green.

If the icon is red, and an Invalid Certificate Detected dialog box appears, click **Verify** and accept the thumbprint of the untrusted certificate, or install a valid CA-signed SSL certificate.

For information about replacing the default certificate for vCenter Server, see the *VMware vSphere Examples and Scenarios* document.

11 Verify that the dashboard icons for the connection server instances are also are green.

If any instances have red icons, click the instance to determine the replication status. Replication might be impaired for any of the following reasons:

- A firewall might be blocking communication
- The VMware VDMDS service might be stopped on a Connection Server instance
- The VMware VDMS DSA options might be blocking the replications
- A network problem has occurred

What to do next

To use a default or self-signed certificate from vCenter Server, see Accept the Thumbprint of a Default TLS Certificate.

If the upgrade fails on one or more of the Connection Server instances, see Create a Replicated Group After Reverting Connection Server to a Snapshot.

Important If you plan to use enhanced message security mode for JMS messages, make sure that firewalls allow Connection Server instances to receive incoming JMS traffic on port 4002 from desktops. Also open port 4101 to accept connections from other Connection Server instances.

If you ever reinstall Connection Server on a server that has a data collector set configured to monitor performance data, stop the data collector set and start it again.

Upgrade to the Latest Version of Connection Server on a Different Machine

As part of your upgrade, you can migrate Connection Server to a new machine.

Prerequisites

- Upgrade at least one existing Connection Server instance to the latest version. See Upgrade Connection Servers in a Replicated Group. During this upgrade, your existing Horizon LDAP will be upgraded.
- Verify that the new physical or virtual machine meets the system requirements for installing Connection Server. See Supported Operating Systems for Horizon Connection Server and Hardware Requirements for Horizon Connection Server.
- Familiarize yourself with the security-related requirements of VMware Horizon, and verify that these requirements are met. See Upgrade Requirements for Horizon Connection Server.
- Determine when to perform this procedure. Choose an available desktop maintenance window. Budget 15 minutes to half an hour for each instance.
- Verify that you have a domain user account with administrative privileges on the host you will use to run the installer.
- Familiarize yourself with the procedure for installing a replicated instance. See the *Horizon Installation* document. You install a replicated instance as part of this procedure.

You do not need to make any changes to the configuration of existing load balancers.

Procedure

1. Verify that an upgraded instance of Connection Server is running and is accessible to the new machine where you plan to install Connection Server.

   When you install Connection Server on the new host, you will point to this existing instance.

2. On the new machine, install a replicated instance of Connection Server.

   The Horizon LDAP on the new instance will replicate that of the upgraded source instance.

3. If applicable, uninstall Connection Server from the old host by using the Windows **Add/ Remove Programs** utility.

4. In Horizon Console, go to **Settings > Servers > Connection Servers** tab and determine whether the Connection Server instance that was uninstalled still appears in the list.

5. If the uninstalled Connection Server instance still appears in the list, use a `vdmadmin` command to remove it.

   ```
   vdmadmin.exe -S -s server_name -r
   ```

   In this example, *server_ name* is the host name or IP address of the Connection Server host. For more information about the `vdmadmin` command-line tool, see the *Horizon Administration* document.

Results

A new instance of Connection Server is added to a group and an old instance is removed.

What to do next

Upgrade the other VMware Horizon server components.

If you ever reinstall Connection Server on a server that has a data collector set configured to monitor performance data, stop the data collector set and start it again.

If you are using load balancers to manage access to Connection Servers, update the load balancer configuration to add the newly installed Connection Servers, and remove the decommissioned Connection Servers (if applicable).

Create a Replicated Group After Reverting Connection Server to a Snapshot

If an upgrade fails, or if for some other reason, you must revert a virtual machine that hosts Connection Server to a snapshot, you must uninstall the other Connection Server instances in the group and recreate the replicated group.

If you revert one Connection Server virtual machine to a snapshot, the Horizon LDAP objects in the database of that virtual machine are no longer consistent with the Horizon LDAP objects in the databases of the other replicated instances. After you revert to a snapshot, the following event is logged in the Windows Event log, in the VMwareVDMDS Event log (Event ID 2103): `The Active Directory Lightweight Directory Services database has been restored using an unsupported restoration procedure`. The reverted virtual machine stops replicating its Horizon LDAP.

If you find it necessary to revert to a snapshot, you must uninstall other Connection Server instances and uninstall the Horizon LDAP database on those virtual machines and then reinstall replica instances.

Prerequisites

Determine which Connection Server instance is to be the new standard, or golden Connection Server. This Connection Server has the desired VMware Horizon configuration data.

Procedure

1. On all Connection Server instances except the one chosen to be the new standard Connection Server instance, uninstall Connection Server and the Horizon LDAP instance.

   The Horizon LDAP database instance is called AD LDS Instance VMwareVDMDS.

2. On the virtual machine that hosts the standard, or golden Connection Server instance, open a command prompt and enter the following command to ensure that replication is not disabled.

   ```
   repadmin /options localhost:389 -DISABLE_OUTBOUND_REPL
   -DISABLE_INBOUND_REPL
   ```

3 On the virtual machines that are to host the replica Connection Server instances, run the Connection Server installer, select the **Replica Server** installation option, and specify the host name or IP address of the standard Connection Server instance.

Results

The replicated group of Connection Server instances is recreated and their Horizon LDAP objects are consistent.

Upgrading Connection Servers in Parallel

If your deployment has multiple Connection Servers, you can upgrade the Connection Servers in parallel to save down time.

Before you perform an upgrade of multiple Connection Servers in parallel, you must verify the following prerequisites.

- Verify that there are no issues with Horizon LDAP replication. For a successful upgrade of multiple Connection Servers in parallel, the local Horizon LDAP instance and the global Horizon LDAP instance in the Connection Server cluster must be in a consistent state. The Connection Server installer blocks the upgrade process if there are any issues with Horizon LDAP replication.

  The local Horizon LDAP instance is created during installation of the first Connection Server and holds configuration data for the Connection Server cluster, which includes the Connection Server and replica servers. This local Horizon LDAP instance is replicated across all Connection Servers within a single cluster.

  The global Horizon LDAP instance is created when you set up the Cloud Pod Architecture environment and holds configuration data for a federation of clusters or pods. This global Horizon LDAP instance is replicated across all Connection Servers in the federation.

  To determine if there are any issues replicating the local Horizon LDAP instance, run the following command:

  ```
  repadmin.exe /showrepl localhost:389
  ```

  To determine if there are any issues replicating the global Horizon LDAP instance in a Cloud Pod Architecture environment, run the following command:

  ```
  repadmin.exe /showrepl localhost:22389
  ```

  For additional troubleshooting information, see Troubleshooting Errors During Upgrade and Installation of Connection Servers.

- Upgrade one Connection Server to determine if there are any issues with Horizon LDAP replication. After you resolve any errors during the upgrade process, you can proceed to upgrade multiple Connection Servers in parallel.

- Bring up all the Horizon LDAP nodes in the Connection Server cluster before the upgrade. This ensures that the schema master node is available on the cluster. The upgrade fails if the schema master node is removed from the cluster. If the schema master node is removed, you can use the `vdmadmin -X` command to make the current node the schema master node. For more information about the `vdmadmin -X` command, see "Detecting and Resolving LDAP Entry and Schema Collisions Using the -X Option" in the *Horizon Administration* document.
- You can upgrade all Connections Servers in three pods at a time.

Use the following process to upgrade all Connection Servers in a pod in parallel:

1 Upgrade all Connection Server instances in the pods. See Upgrade Connection Servers in a Replicated Group.

Note The Connection Server installer will pause for a longer time than usual at the last step because it waits for all the services to start.

Troubleshooting Errors During Upgrade and Installation of Connection Servers

The Connection Server installer has certain restrictions that can block the Connection Server installation process when you upgrade Connection Servers in parallel. These restrictions also apply to individual Connection Server upgrades and fresh installations of replica servers.

Problem

When you run the Connection Server installers while performing an upgrade or installation of Connection Servers, the Connection Server installer can display error messages and block the installation process.

Cause

Connection Server installation or upgrade errors can occur when the schema master node is not available or is removed from the LDAP cluster. The schema master node is deleted when a Connection Server instance is removed using the `vdmadmin -S` command without a clean uninstallation of LDAP instances.

Solution

1 If the installation error occurs due to the unavailability of the schema master node, bring up all nodes in the LDAP cluster specified in the error message.

If bringing up all nodes in the LDAP cluster does not resolve the issue, then the error can occur because the schema master node is removed from the cluster. Proceed to Step 2 to troubleshoot the error.

2 If the schema master node is removed from the LDAP cluster, you must make another node the schema master node on the cluster. The steps to make another node the schema master node on the cluster are based on whether any or none of the nodes are upgraded to VMware Horizon version 2006 on the cluster.

- If any node is upgraded to VMware Horizon version 2006 on the cluster, then you can use the `vdmadmin -X` command to make the current node the schema master node. For more information about the `vdmadmin -X` command, see "Detecting and Resolving LDAP Entry and Schema Collisions Using the -X Option" in the *Horizon Administration* document.
  - To make the current node the schema master node on the cluster for a local LDAP instance, enter the following command:

    ```
    vdmadmin -X -seizeSchemaMaster
    ```

  - To Make the current node the schema master node on the cluster for a global LDAP instance in a Cloud Pod Architecture environment, enter the following command.

    ```
    vdmadmin -X -seizeSchemaMaster -global
    ```

- If none of the nodes are upgraded to VMware Horizon version 2006 on the cluster, then use the `dsmgmt` command to make the current node the schema master node.
  - To make the current node the schema master node on the cluster for a local LDAP instance, enter the following command:

    ```
    dsmgmt "roles" "connections" "connect to server localhost:389" "quit" "transfer
    schema master" "quit" "quit"
    ```

  - To make the current node the schema master node on the cluster for a global LDAP instance, enter the following command:

    ```
    dsmgmt "roles" "connections" "connect to server localhost:22389" "quit" "transfer
    schema master" "quit" "quit"
    ```

Upgrading Enrollment Servers

You can upgrade an enrollment server by running the latest version of the Connection Server installer on the virtual machine that already has an earlier version of an enrollment server installed. Or, you can uninstall the earlier version of an enrollment server and install the latest version by running the latest version of the Connection Server installer and selecting the Enrollment Server option.

An enrollment server is stateless. The configuration related to True SSO does not get persisted on the enrollment server. The enrollment server receives the True SSO configuration from Connection Server when the enrollment server is running and the Connection Server successfully connects to the enrollment server.

Note After upgrading you do not need to manually import the pairing certificate(s) from the Connection Server to the enrollment server's Windows Certificate Store again. The pairing certificate(s) manually imported earlier are not removed as part of the uninstall or upgrade process. When the enrollment server is running after an upgrade, the Connection Server is able to successfully connect and the previously imported pairing certificate(s) are reused.

Upgrading a Cloud Pod Architecture Environment

The Cloud Pod Architecture feature uses standard Horizon components to provide cross-data center administration. With the Cloud Pod Architecture feature, you link together multiple pods to provide a single large desktop and application brokering and management environment. A pod consists of a set of Connection Server instances, shared storage, a database server, and the vSphere and network infrastructures required to host desktop and application pools.

Use the following process to upgrade a Cloud Pod Architecture environment.

1 Upgrade all Connection Server instances in one pod, according to the usual process for upgrading a single Connection Server instance.

2 Repeat the preceding step for the other pods in the pod federation, upgrading each pod one-by-one.

During the upgrade process, some Connection Server instances use the latest version of VMware Horizon and some use the older version. Although this mixed-version environment is supported beginning with Horizon 7 version 7.4, new features do not work in a mixed environment. For example, a new feature that is visible in Horizon Console on an upgraded server is not visible in Horizon Console on a server that has not been upgraded.

For information about designing and setting up a Cloud Pod Architecture environment, see *Administering Cloud Pod Architecture in Horizon*.

Upgrading VMware HorizonServers to Allow HTML Access

When upgrading Connection Server instances behind a load balancer or behind a gateway such as Unified Access Gateway, you must make configuration changes to continue to use HTML Access.

For more information, see "Allow HTML Access Through a Load Balancer" and "Allow HTML Access Through a Gateway" in the *Horizon Installation* document.

Upgrade vCenter Server

Perform a vCenter Server upgrade as part of the same maintenance window during which you upgrade other VMware Horizon server components. Before you upgrade vCenter Server, you must back up some VMware Horizon data.

Note During the vCenter Server upgrade, existing remote desktop and application sessions will not be disconnected, but the following functionality is not available during the vCenter Server upgrade:

- Remote desktops that are in a provisioning state will not get powered on.
- New desktops cannot be launched.

Prerequisites

- Determine when to perform this procedure. Choose an available desktop maintenance window. For information about how much time is required, see the *VMware vSphere Upgrade Guide*.
- Back up the vCenter Server database.
- Back up the Horizon Directory database from a Connection Server instance by using the `vdmexport.exe` utility.

  For instructions, see the *Horizon Administration* document. If you have multiple instances of Connection Server in a replicated group, you need to export the data from only one instance.
- Verify that the server on which vCenter Server is installed has a CA (certificate authority)-signed TLS server certificate installed and configured. After you upgrade Connection Server, if vCenter Server does not use a CA-signed certificate, the default self-signed certificate is shown as invalid in Horizon Console, and a message indicates that vCenter Server is unavailable.
- Complete the prerequisites listed in the *VMware vSphere Upgrade Guide*, using the version of the guide that corresponds to the version of vSphere that you plan to upgrade to.
- To upgrade vCenter Server while instant clones are in use, see the steps in the VMware Knowledge Base (KB) article https://kb.vmware.com/s/article/52573.

Procedure

1 Upgrade vCenter Server as described in the *VMware vSphere Upgrade Guide*.

  Important If your clusters contain vSAN datastores, also see the chapter about upgrading the vSAN cluster, in the *Administering VMware vSAN* document. This chapter contains a topic about upgrading vCenter Server.

2 Log in to Horizon Console and examine the dashboard to verify that the vCenter Server icon is green.

   If this icon is red and an Invalid Certificate Detected dialog box appears, you must click **Verify** and either accept the thumbprint of the untrusted certificate, as described in "What to Do Next," or install a valid CA-signed SSL certificate.

   For information about replacing the default certificate for vCenter Server, see the *VMware vSphere Examples and Scenarios* document.

What to do next

To use a default or self-signed certificate from vCenter Server, see Accept the Thumbprint of a Default TLS Certificate.

If you have finished upgrading VMware Horizon server components, at your next maintenance window, continue with the VMware Horizon upgrade.

- If you are also upgrading vSphere components, see Chapter 6 Upgrade ESXi Hosts and Their Virtual Machines.
- If you upgrading only VMware Horizon components, see Upgrade Horizon Agent.

Accept the Thumbprint of a Default TLS Certificate

When you add vCenter Server instances to VMware Horizon, you must ensure that the TLS certificates that are used for vCenter Server are valid and trusted by Connection Server. If the default certificates that are installed with vCenter Server are still in place, you must determine whether to accept these certificates' thumbprints.

If a vCenter Server is configured with a certificate that is signed by a CA, and the root certificate is trusted by Connection Server, you do not have to accept the certificate thumbprint. No action is required.

If you replace a default certificate with a certificate that is signed by a CA, but Connection Server does not trust the root certificate, you must determine whether to accept the certificate thumbprint. A thumbprint is a cryptographic hash of a certificate. The thumbprint is used to quickly determine if a presented certificate is the same as another certificate, such as the certificate that was accepted previously.

For details about configuring TLS certificates, see "Configuring TLS Certificates for VMware Horizon Servers" in the *Horizon Installation* document.

You first add vCenter Server in Horizon Console by using the Add vCenter Server wizard. If a certificate is untrusted and you do not accept the thumbprint, you cannot add vCenter Server.

After these servers are added, you can reconfigure them in the Edit vCenter Server dialog box.

Note You also must accept a certificate thumbprint when you upgrade from an earlier release and a vCenter Server certificate is untrusted, or if you replace a trusted certificate with an untrusted certificate.

On the Horizon Console dashboard, the vCenter Server icon turns red and an Invalid Certificate Detected dialog box appears. In Horizon Console, click **Settings > Servers** and select the vCenter Server. Then, click **Edit** in the vCenter Server settings and follow the prompts to verify the and accept the self-signed certificate.

Similarly, in Horizon Console you can configure a SAML authenticator for use by a Connection Server instance. If the SAML server certificate is not trusted by Connection Server, you must determine whether to accept the certificate thumbprint. If you do not accept the thumbprint, you cannot configure the SAML authenticator in VMware Horizon. After a SAML authenticator is configured, you can reconfigure it in the Edit Connection Server dialog box.

Procedure

1. When Horizon Console displays an Invalid Certificate Detected dialog box, click **View Certificate**.
2. Examine the certificate thumbprint in the Certificate Information window.
3. Examine the certificate thumbprint that was configured for the vCenter Server .
   a. On the vCenter Server host, start the MMC snap-in and open the Windows Certificate Store.
   b. Navigate to the vCenter Server certificate.
   c. Click the Certificate Details tab to display the certificate thumbprint.

   Similarly, examine the certificate thumbprint for a SAML authenticator. If appropriate, take the preceding steps on the SAML authenticator host.
4. Verify that the thumbprint in the Certificate Information window matches the thumbprint for the vCenter Server.

   Similarly, verify that the thumbprints match for a SAML authenticator.
5. Determine whether to accept the certificate thumbprint.

Option	Description
The thumbprints match.	Click **Accept** to use the default certificate.
The thumbprints do not match.	Click **Reject**. Troubleshoot the mismatched certificates. For example, you might have provided an incorrect IP address for vCenter Server.

Using Horizon Group Policy Administrative Template Files

Horizon provides several component-specific Group Policy Administrative ADMX template files. You can optimize and secure remote desktops and applications by adding the policy settings in the ADMX template files to a new or existing GPO in Active Directory.

All ADMX files that provide group policy settings for Horizon are available in `VMware-Horizon-Extras-Bundle-YYMM-x.x.x-yyyyyyyy.zip`, where *YYMM* is the marketing version, *x.x.x* is the internal version and *yyyyyyyy* is the build number. You can download the file from the VMware Downloads site at https://my.vmware.com/web/vmware/downloads. Under Desktop & End-User Computing, select the VMware Horizon download, which includes the GPO Bundle containing the ZIP file.

To upgrade group policies, use the Group Policy Object Editor on your Active Directory server to add the new version of the template files.

The Horizon ADMX template files contain both Computer Configuration and User Configuration group policies.

- The Computer Configuration policies set policies that apply to all remote desktops, regardless of who connects to the desktop.
- The User Configuration policies set policies that apply to all users, regardless of the remote desktop or application they connect to. User Configuration policies override equivalent Computer Configuration policies.

Microsoft Windows applies policies at desktop startup and when users log in.

Upgrade ESXi Hosts and Their Virtual Machines

6

Upgrading ESXi hosts and virtual machines is the most time-consuming aspect of this middle phase of a VMware Horizon upgrade.

This procedure provides an overview of the tasks you must perform during the second and subsequent maintenance windows. To complete some of these tasks, you might need step-by-step instructions found in the *VMware vSphere Upgrade Guide* and the *Horizon Administration* document.

For details about which versions of Horizon are compatible with which versions of vCenter Server and ESXi, see the VMware Product Interoperability Matrix at http://www.vmware.com/resources/compatibility/sim/interop_matrix.php.

Prerequisites

- Complete the procedure described in Upgrade Connection Servers in a Replicated Group.
- Perform the ESXi upgrade preparation tasks listed in the *VMware vSphere Upgrade Guide*.

Procedure

1 Upgrade ESXi hosts, cluster by cluster.

For instructions, see the *VMware vSphere Upgrade Guide*. If your clusters contain vSAN datastores, also see the chapter about upgrading the vSAN cluster, in the *Administering VMware vSAN* document. This chapter contains a topic about upgrading ESXi hosts.

If you have many clusters, this step could take several maintenance windows to complete. Upgrading ESXi hosts might include the following tasks:

a Use VMware vSphere® vMotion® to move the virtual machines off of the ESXi host.

b Put the host into maintenance mode.

c Perform the upgrade.

d Use VMotion to move the virtual machines back onto the host.

e Perform post-upgrade tasks for ESXi hosts.

Every host must be a member of a cluster, as mentioned in the prerequisites.

2 If an upgraded host does not reconnect itself to vCenter Server, use vSphere Client to reconnect the host to vCenter Server.

3 (Optional) Upgrade VMware® Tools™ and the virtual machines on all golden images, virtual machine templates, and virtual machines that host VMware Horizon server components such as Connection Server instances.

   a Plan for down time, as described in the *VMware vSphere Upgrade Guide*.

   b Update VMware Tools, and upgrade the virtual machine hardware for virtual machines that will be used as sources for remote desktops.

   For step-by-step instructions if you plan not to use VMware vSphere® Update Manager™, see the chapter about upgrading virtual machines in the *VMware vSphere Virtual Machine Administration* document.

   If you use VMware vSphere Update Manager, you can update VMware Tools and then the virtual hardware version in the correct order for all the virtual machines in a particular folder. See the *VMware vSphere Upgrade Guide*.

4 (Optional) If you use full-clone desktops, on each virtual machine, upgrade VMware Tools and the virtual hardware for virtual machines that will be used as sources for remote desktops.

   For step-by-step instructions if you plan not to use VMware vSphere® Update Manager™, see the chapter about upgrading virtual machines in the *VMware vSphere Virtual Machine Administration* document.

   If you use vSphere Update Manager, you can update VMware Tools and then the virtual hardware version in the correct order for all the virtual machines in a particular folder. See the *VMware vSphere Upgrade Guide*.

What to do next

Upgrade the agent software. See Upgrade Horizon Agent.

Upgrading Published and Virtual Desktops 7

Upgrade published desktops, virtual desktops and Horizon Agent, which runs inside the operating systems of virtual desktops or published desktops and Microsoft RDS hosts.

Important This chapter does not contain information about upgrading Horizon Agent on a Linux virtual machine. For this information, see the *Setting Up Linux Desktops in Horizon* document.

The strategy for upgrading on the type of desktop source:

- For an automated pool of full clone desktops, you must upgrade Horizon Agent individually in each virtual desktop. You will also need to upgrade Horizon Agent in the template VM you used to create the full-clone desktops. In the event that you expand the pool, additional desktops will be created using the updated template VM.
- For a manual pool of vCenter virtual machines, non-vCenter virtual machines, and physical PCs, you must upgrade Horizon Agent individually in each machine.
- For an automated pool of instant-clone desktops, you must upgrade Horizon Agent on the golden image. Then, you can propagate the new golden image across the instant-clone desktop pool by performing a push-image operation.
- For a RDS desktop pool, you must upgrade Horizon Agent on one or more Terminal Services host or Microsoft RDS host. See Upgrade RDS Hosts That Provide Session-Based Desktops.

This chapter includes the following topics:

Upgrade Horizon Agent

You must upgrade Horizon Agent on the golden image for an instant-clone desktop pool.

This procedure provides an overview of the tasks you must perform to upgrade the agent software in virtual machines used as desktop sources. To complete some of these tasks, you might need the step-by-step instructions found in the vSphere Client online help or in *Setting Up Virtual Desktops in Horizon*, available by clicking the **Help** button in Horizon Administrator. To upgrade the agent software on a Terminal Services host or Microsoft RDS host, see Upgrade RDS Hosts That Provide Session-Based Desktops. To upgrade the agent software on a Linux virtual machine, see the *Setting Up Linux Desktops in Horizon* document.

If you plan to deploy instant clones, you can use this procedure to create a golden image for an instant-clone desktop pool. When you upgrade Horizon Agent on a golden image, simply select the appropriate option for an instant-clone desktop pool.

Prerequisites

- Verify that all Connection Server instances in the replicated group have been upgraded. All Connection Server instances must be upgraded first so that the secure JMS pairing mechanism can work with Horizon Agent.
- If you are upgrading ESXi hosts and virtual machines, complete the procedure described in Chapter 6 Upgrade ESXi Hosts and Their Virtual Machines.
- Verify that you have a domain user account with administrative privileges on the hosts that you use to run the installer and perform the upgrade.

Procedure

1. Upgrade the agent software on a golden image or VM template and create an instant-clone desktop pool or full-clone desktop pool, depending on your use case for testing purposes. Or, if you are using a manual desktop pool, test it on one desktop in the pool.
   a. Download and run the new version of the Horizon Agent installer on the golden image or VM template.

      You can download the installer from the VMware website.

   b. Create a small desktop pool from this virtual machine.

   c. Test a virtual machine desktop from the desktop pool to verify that all the use cases function properly.

      For example, create a desktop pool that contains one virtual machine desktop, and verify that you can use Horizon Client to log in to that desktop.

   Step-by-step instructions for running the Horizon Agent installer and creating desktop pools appear in *Setting Up Virtual Desktops in Horizon*, available by clicking the **Help** button in Horizon Console.
2. Repeat Step 1 on all your golden images and virtual machine templates.

3 If you plan to create instant-clone desktop pools, take a snapshot of each upgraded golden image.

   Go to the pool you want to upgrade and perform a push-image operation. For more information on performing a push image operation, see the *Setting Up Virtual Desktops in Horizon* document.

   For instructions on taking snapshots, see the vSphere Client online help.

4 If you use an automated desktop pool of full clones or a manual desktop pool, upgrade the agent software on each virtual desktop by using whatever third-party tools you usually use for software upgrades.

   If your desktop pool is an automated full-clone desktop pool, take a snapshot of the new VM template. If you later expand your pool, new virtual desktops will be created from the updated VM template or snapshot.

5 For non-instant-clone pools, to turn on the 3D rendering feature, edit the pool settings.

   a Configure the following pool settings:

      - For Windows desktop pools, set the pool to use the PCoIP display protocol or the VMware Blast display protocol. For Linux desktop pools, set the pool to use the VMware Blast display protocol.
      - Set **Allow users to choose protocol** to **No**.
      - For Windows desktop pools, turn on the **3D Renderer** feature. For Linux desktop pools, select **NVIDIA GRID vGPU** if you have configured that vGPU, or select **Manage using vSphere Client**.

   b For Windows desktop pools only, power off each virtual machine and power it on again.

      Restarting a virtual machine, rather than powering off and on, does not cause the setting to take effect.

6 Download and run the installer for the new version of Horizon Agent on all the machines that you use as RDS hosts. In Windows, RDS hosts can be physical PCs or virtual machines. In Linux, only virtual machines can serve as RDS hosts.

   You can download the installer from the VMware website.

   Important When you run the installer on a Windows virtual machine RDS host, the **View Composer Agent** component is deselected. Do not select this component during an upgrade.

7 For Windows desktop pools, if you use physical PCs as desktop sources, download and run the installer for the new version of Horizon Agent on these physical machines.

   You can download the installer from the VMware website.

   Important On Windows Server operating systems configured for desktop use, if you do not want to change Horizon Agent installation mode during upgrade, select **Desktop Mode** in Horizon Agent installer and proceed. If you want to change the mode, select **RDS Mode** and follow the installer instructions to proceed with upgrade.

8 Use a Horizon Client that has not been upgraded to verify that you can log in to the upgraded remote desktop sources with your old client software.

Upgrade Instant-Clone Desktop Pools When You Upgrade vCenter Server to vSphere 6.7 or Later

vSphere 6.7 has a new API for instant clones. Therefore, if you are using instant clones, and are upgrading from a vSphere version earlier than 6.7 to vSphere 6.7 or later, you must complete the steps in this upgrade process. For example, if you are upgrading from vSphere 6.0 to vSphere 6.7, from vSphere 6.5 to vSphere 6.7, or from vSphere 6.5 to vSphere 7.0, this process applies. This process does not apply if you are upgrading from vSphere 6.7 to vSphere 7.0.

Prerequisites

- Complete the system requirements for an upgrade to VMware Horizon 2006 or later.
- Complete procedures described in Upgrading Horizon Connection Server.
- Complete the procedure described in Upgrade Horizon Agent for upgrading the agent in the golden image.
- Complete the prerequisites listed in the *VMware vSphere Upgrade Guide*, using the version of the guide that corresponds to the version of vSphere that you plan to upgrade to.

  Note If you upgrade vCenter Server to vSphere 6.7 or later, then all or some of the ESXi hosts in the cluster must be upgraded to the newer version. Else, the instant-clone desktop pools will not be provisioned properly.

- Identify the ESXi hosts that you plan to upgrade and verify that you leave enough hosts online for existing desktop pools.

Procedure

1 Take a snapshot of the golden image on which you upgrade Horizon Agent to VMware Horizon 2006 or later.

2 Set the Storage Distributed Resource Scheduler (DRS) migration threshold to 3 in the cluster.

3 Disable the instant-clone desktop pools.

4 Upgrade vCenter Server to vSphere 6.7 or later.

5 To put the hosts that you plan to upgrade into maintenance mode, choose one of the following options.

   - Put the host directly into maintenance mode from vSphere Client then upgrade the host to vSphere 6.7 or later. After the upgrade completes, use vSphere Client to exit maintenance mode.
   - Use the `icmaint.cmd` utility to mark a host for maintenance with the **ON** option. Marking a host for maintenance deletes the golden images, which are the parent VMs in vCenter Server from the ESXi host. Put the host into maintenance mode and upgrade to the new ESXi version. After the upgrade completes, exit the host from maintenance mode. Then, use the `icmaint.cmd` to unmark the host for maintenance with the **OFF** option.

   Note You must upgrade at least one host so that you can resume the provisioning of desktop pools. Then you must upgrade all the other hosts.

6 Enable the instant-clone desktop pools.

7 Perform a push-image operation for each instant-clone desktop pool that uses the new snapshot.

   Only the hosts that are upgraded to the newer ESXi version are used for provisioning. The instant clones created during the push-image operation might be migrated to other hosts that are not yet on the new vSphere version.

8 Verify that all hosts in the cluster are upgraded to the new vSphere version.

9 If you upgrade the golden image from a previous version to be compatible with ESXi 6.7 and later (VM version 14), then upgrade VMware Tools on the golden image. You must take a new snapshot of the golden image that Horizon uses to perform a push-image operation on all the instant-clone desktop pools that used the previous version of this golden image.

10 If the Virtual Distributed Switch (vDS) is upgraded, power on the golden image on to verify that there are no network issues. Following a vDS upgrade, you must take a new snapshot of the golden image and perform a push-image operation on all the instant-clone desktop pools.

Upgrade RDS Hosts That Provide Session-Based Desktops

On RDS hosts with Windows Server 2012 R2 or a later operating system, you can upgrade the Horizon Agent software and edit pool settings so that the RDS host can provide remote desktops and remote Windows-based applications.

Prerequisites

- Verify that at least one Horizon Connection Server instance in the replicated group has been upgraded. Connection Server must be upgraded first so that the secure JMS pairing mechanism can work with Horizon Agent.

- Verify that the RDS host currently hosting remote desktops is running a supported version of Windows Server operating systems. If you do not have a supported Windows Server operating system, you must do a fresh installation rather than an upgrade. For a list of supported operating systems, see Requirements and Considerations for Horizon Agent.
- Verify that the RDS Host role is installed in the operating system. See the procedure called "Install Remote Desktop Services" in the *Setting Up Published Desktops and Applications in Horizon* document.
- Familiarize yourself with the procedure for running the Horizon Agent installer. See the procedure called "Install Horizon Agent on a Remote Desktop Services Host," in *Setting Up Published Desktops and Applications in Horizon*, available by clicking the **Help** button in Horizon Console.
- Verify that you have logged off from all remote desktops and remote applications.
- Verify that you have a domain user account with administrative privileges on the hosts that you use to run the installer and perform the upgrade.

Procedure

1. In Horizon Console, edit the desktop pool settings for the pool to disable the pool.

   Go to **Inventory > Desktops**, select the pool, and click **Edit**.
2. On the RDS host, download and run the installer for the new version of Horizon Agent.

   You can download the installer from the VMware Web site.
3. In Horizon Console, edit the farm settings and set the default display protocol to **PCoIP** or **VMware Blast**.

   Go to **Inventory > Farms**, select the farm, and click **Edit**.

   You can also use a setting that allows the end user to choose the protocol. To use remote applications, the protocol must be PCoIP or VMware Blast. Remote applications are not supported with RDP.
4. In Horizon Console, edit the desktop pool settings for the pool to enable the pool.

Results

This host can now provide remote applications in addition to remote desktops. In Horizon Console, if you go to **Inventory > Desktops**, you see that the type of pool is **RDS Desktop Pool**. If you go to **Inventory > Farms**, you see a farm ID in the list that corresponds to the pool ID.

Upgrading vSphere Components Separately in a VMware Horizon Environment

8

If you upgrade vSphere components separately from VMware Horizon components, you must back up some VMware Horizon data and reinstall some VMware Horizon software.

Instead of performing an integrated upgrade of VMware Horizon and vSphere components, you can choose to first upgrade all VMware Horizon components and then upgrade vSphere components, or the reverse. You might also upgrade only vSphere components when a new version or update of vSphere is released.

When you upgrade vSphere components separately from VMware Horizon components, you must perform the following additional tasks:

1 Before you upgrade vCenter Server, back up the vCenter Server database.

2 Before you upgrade vCenter Server, back up the Horizon Directory database from a Horizon Connection Server instance by using the `vdmexport.exe` utility.

   For instructions, see the *Horizon Administration* document. If you have multiple instances of Connection Server in a replicated group, you need to export the data from only one instance.