Horizon Installation and Upgrade

VMware Horizon 2209

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

Horizon Installation and Upgrade

This guide explains how to install and upgrade the VMware Horizon 8® server, agent, and client components.

Intended Audience

This information is intended for anyone who wants to install VMware Horizon 8 or upgrade to this latest version of the product. The information is written for experienced Windows or Linux system administrators who are familiar with virtual machine technology and datacenter operations.

System Requirements for Server Components

1

Hosts and virtual machines that run VMware Horizon 8 server components must meet specific hardware and software requirements.

Many of these requirements are identical for both VMware Horizon 8 installations and upgrades.

This chapter includes the following topics:

- Horizon Connection Server Requirements
- Horizon Console Requirements - Install Only
- Compatibility Matrix for Various Versions of VMware Horizon 8Components - Upgrade Only

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 - Install and Upgrade

  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.

- Supported Operating Systems for Horizon Connection Server- Install and Upgrade

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

- Virtualization Software Requirements for Horizon Connection Server - Install Only

  If you choose to deploy VMware Horizon 8 in a VMware virtualized environment some minimum version of the virtualization software is required.

- Network Requirements for Replicated Horizon Connection Server Instances - Install Only

  When installing replicated Horizon Connection Server instances, you must usually configure the instances in the same physical location and connect them over a high-performance LAN. Connection Server instances must be located on the same L2 network and broadcast domain.

- Upgrade Requirements for Horizon Connection Server

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

Hardware Requirements for Horizon Connection Server - Install and Upgrade

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 1-1. 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- Install and Upgrade

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.

Virtualization Software Requirements for Horizon Connection Server - Install Only

If you choose to deploy VMware Horizon 8 in a VMware virtualized environment some minimum version of the virtualization software is required.

If you are using vSphere, you must use a supported version of vSphere ESX/ESXi hosts and vCenter Server.

For details about which versions of VMware Horizon 8 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.

Network Requirements for Replicated Horizon Connection Server Instances - Install Only

When installing replicated Horizon Connection Server instances, you must usually configure the instances in the same physical location and connect them over a high-performance LAN. Connection Server instances must be located on the same L2 network and broadcast domain.

Important To use a group of replicated Connection Server instances across a WAN, MAN (metropolitan area network), or other non-LAN, in scenarios where a VMware Horizon 8 deployment needs to span data centers, you must use the Cloud Pod Architecture feature. For more information, see the *Cloud Pod Architecture in Horizon* document.

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 8 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 8 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 8 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 and Upgrade* guide.

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 and Upgrade* 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 and Upgrade* 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 and Upgrade* document.

Horizon Console Requirements - Install Only

Administrators use Horizon Console to configure Horizon Connection Server, deploy and manage remote desktops and applications, control user authentication, initiate and examine system events, and carry out analytical activities. Client systems that run Horizon Console must meet certain requirements.

Horizon Console is a web-based application that is installed when you install Connection Server. You can access and use Horizon Console with the following web browsers:

- Firefox (latest versions)
- Chrome (latest versions)
- Safari (latest versions)
- Microsoft Edge (Windows 10)

Note If using an older Web browser to launch Horizon Console, a message appears indicating that using a modern browser will provide a better user experience. You can click on your preferred Web browser from the options displayed to download it. Note that the Internet Explorer browser is no longer supported for accessing Horizon Console.

The computer on which you launch Horizon Console must trust the root and intermediate certificates of the server that hosts Connection Server. The supported browsers already contain certificates for all of the well-known certificate authorities (CAs). If your certificates come from a CA that is not well known, you must follow the instructions in Configure Client Endpoints to Trust Root and Intermediate Certificates.

To display text properly, Horizon Console requires Microsoft-specific fonts. If your web browser runs on a non-Windows operating system such as Linux, UNIX, or Mac, make sure that Microsoft-specific fonts are installed on your computer.

Currently, the Microsoft web site does not distribute Microsoft fonts, but you can download them from independent web sites.

Compatibility Matrix for Various Versions of VMware Horizon 8Components - Upgrade Only

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 8:

- 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 1-2. Compatibility Matrix for VMware Horizon 8 2006 or Later and Earlier Versions of VMware Horizon 8 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 VMware Horizon 8 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.

System Requirements for Guest Operating Systems

2

Systems running Horizon Agent must meet certain hardware and software requirements.

This chapter includes the following topics:

Requirements and Considerations for Horizon Agent - Install and Upgrade

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 Disable Weak Ciphers in SSL/TLS.

Remote Display Protocol and Software Support - Install Only

Remote display protocols and software provide access to remote desktops and applications. The remote display protocol used depends on the type of client device, whether you are connecting to a remote desktop or a remote application, and how the administrator configures the desktop or application pool.

For information about which desktop operating systems support specific remote display protocol features, see the *Horizon Overview and Deployment Planning* document.

For information about which client devices support specific remote display protocol features, go to https://docs.vmware.com/en/VMware-Horizon-Client/index.html.

Preparing Active Directory

3

VMware Horizon 8 uses your existing Microsoft Active Directory infrastructure for user authentication and management. You must perform certain tasks to prepare Active Directory for use with VMware Horizon 8.

VMware Horizon 8 supports certain Active Directory Domain Services (AD DS) domain functional levels. For more information, see the VMware Knowledge Base (KB) article https://kb.vmware.com/s/article/78652.

This chapter includes the following topics:

Support for Azure Active Directory

VMware Horizon supports limited deployment and Horizon pool types for Azure Active Directory.

Supported Azure AD deployment types

Only the Hybrid Azure AD deployment, where the on-prem Active directory is connected to Azure AD is supported. To connect your on-prem Active Directory to Azure AD, please refer to the Microsoft Azure AD documentation.

Supported Horizon pool types

Only the Manual and Automated full clone desktop pools are supported.

Single Sign-On into Azure AD assigned resources will not work until the desktop VM is in a state where it can issue an Azure AD Primary Refresh Token (PRT) on the end user login. See the Microsoft Azure AD documentation to learn more about Azure AD PRT.

Best Practices

- If you do not select computer accounts, then on the deletion or rebuild of any pool VM the newly created VM uses a different VM name and adds a new device account in Active directory. The old device entry, which is no longer useful, remains in AD. To avoid this situation, select the "Allow Reuse of Existing Computer Accounts" check box when creating a full clone pool.
- When the desktop pool is deleted from Horizon 8, computer accounts are not removed from the AD. The Administrator must remove them from the Active Directory.

Configuring Domains and Trust Relationships

You must join each Connection Server host to an Active Directory domain. The host must not be a domain controller.

Active Directory also manages the Horizon Agent machines, including single-user machines and RDS hosts, and the users and groups in your VMware Horizon 8 deployment. You can entitle users and groups to remote desktops and applications, and you can select users and groups to be administrators in VMware Horizon 8.

You can place Horizon Agent machines and users and groups, in the following Active Directory domains:

- The Connection Server domain
- A different domain that has a two-way trust relationship with the Connection Server domain
- A domain in a different forest than the Connection Server domain that is trusted by the Connection Server domain in a one-way external or realm trust relationship
- A domain in a different forest than the Connection Server domain that is trusted by the Connection Server domain in a one-way or two-way transitive forest trust relationship
- Untrusted domains

Users are authenticated using Active Directory against the Connection Server domain, any additional user domains with which a trust agreement exists, and untrusted domains.

If your users and groups are in one-way trusted domains, you must provide secondary credentials for the administrator users in Horizon Console. Administrators must have secondary credentials to give them access to the one-way trusted domains. A one-way trusted domain can be an external domain or a domain in a transitive forest trust.

Secondary credentials are required only for Horizon Console sessions, not for end users' desktop or application sessions. Only administrator users require secondary credentials.

You can provide secondary credentials by using the `vdmadmin -T` command.

- You configure secondary credentials for individual administrator users.
- For a forest trust, you can configure secondary credentials for the forest root domain. Connection Server can then enumerate the child domains in the forest trust.

For more information, see "Providing Secondary Credentials for Administrators Using the -T Option" in the *Horizon Administration* document.

Smart card and SAML authentication of users is not supported in one-way trusted domains.

Unauthenticated access is not supported in a one-way trust environment when authenticating a user from a trusted domain. For example, there are two domains, Domain A and Domain B, where Domain B has a one-way outgoing trust to Domain A. When you enable unauthenticated access on the Connection Server in Domain B and add an unauthenticated access user from a user list in Domain A and then entitle the unauthenticated user to a published desktop or application pool, the user cannot log in as an unauthenticated access user from Horizon Client.

The Logon as current user feature in Horizon Client for Windows is supported in one-way trusted domains.

Untrusted Domains

A domain in a different forest than the Connection Server domain that does not have any formal trust with the Connection Server domain is an untrusted domain relationship. For an untrusted domain relationship, users are authenticated using the primary domain bind account credentials. Users can be authenticated with auxiliary domain bind accounts only if the primary domain bind account is inaccessible. For more information about configuring untrusted domains, see "Configuring Untrusted Domains" in the *Horizon Administration* document.

The following features are not supported in an untrusted domain:

- Logon as current user
- vdmadmin commands
- Adding an administrator user for an untrusted domain
- IPv6
- Identify an AD User That Does Not Have an AD UPN

Trust Relationships and Domain Filtering

To determine which domains it can access, a Connection Server instance traverses trust relationships beginning with its own domain.

For a small, well-connected set of domains, Connection Server can quickly determine the full list of domains, but the time that it takes increases as the number of domains increases or as the connectivity between the domains decreases. The list might also include domains that you would prefer not to offer to users when they connect to their remote desktops and applications.

You can use the `vdmadmin` command to configure domain filtering to limit the domains that a Connection Server instance searches and that it displays to users. See the *Horizon Administration* document for more information.

If a forest trust is configured with name suffix exclusions, the configured exclusions are used to filter the list of forest child domains. Name suffix exclusion filtering is applied in addition to the filtering that is specified with the `vdmadmin` command.

Creating an OU for Remote Desktops

You should create an organizational unit (OU) specifically for your remote desktops. An OU is a subdivision in Active Directory that contains users, groups, computers, or other OUs.

To prevent group policy settings from being applied to other Windows servers or workstations in the same domain as your desktops, you can create a GPO for your VMware Horizon 8 group policies and link it to the OU that contains your remote desktops. You can also delegate control of the OU to subordinate groups, such as server operators or individual users.

Creating OUs and Groups for Kiosk Mode Client Accounts

A client in kiosk mode is a thin client or a locked-down PC that runs the client software to connect to a Connection Server instance and launch a remote desktop session. If you configure clients in kiosk mode, you should create dedicated OUs and groups in Active Directory for kiosk mode client accounts.

Creating dedicated OUs and groups for kiosk mode client accounts partitions client systems against unwarranted intrusion and simplifies client configuration and administration.

See the *Horizon Administration* document for more information.

Creating Groups for Users

You should create groups for different types of users in Active Directory. For example, you can create a group called VMware Horizon 8 Users for your end users and another group called VMware Horizon 8 Administrators for users that will administer remote desktops and applications.

Creating a User Account for vCenter Server

You must create a user account in Active Directory to use with vCenter Server. You specify this user account when you add a vCenter Server instance in Horizon Console.

You must give the user account privileges to perform certain operations in vCenter Server. You can create a vCenter Server role with the appropriate privileges and assign the role to the vCenter Server user. The list of privileges you add to the vCenter Server role varies, depending on whether you use VMware Horizon 8with or without instant clones. See Configuring User Accounts for vCenter Server.

Create a User Account for Instant-Clone Operations

Before you deploy instant clones, you must create a user account that has the permission to perform certain operations in Active Directory.

Select this account when you add an instant-clone domain administrator before deploying instant-clone desktop pools. For more information, see Add an Instant-Clone Domain Administrator.

Procedure

1. In Active Directory, create a user account in the same domain as the Connection Server or in a trusted domain.
2. Add the **Create Computer Objects**, **Delete Computer Objects**, and **Write All Properties** permissions to the account on the container for the instant-clone computer accounts.

   The following list shows the required permissions for the user account, including permissions that are assigned by default:

   - List Contents
   - Read All Properties
   - Write All Properties
   - Read Permissions
   - Reset Password
   - Create Computer Objects
   - Delete Computer Objects

   Make sure that the permissions apply to the correct container and to all child objects of the container.

Configure the Restricted Groups Policy

To be able to connect to a remote desktop, users must belong to the local Remote Desktop Users group of the remote desktop. You can use the Restricted Groups policy in Active Directory to add users or groups to the local Remote Desktop Users group of every remote desktop that is joined to your domain.

The Restricted Groups policy sets the local group membership of computers in the domain to match the membership list settings defined in the Restricted Groups policy. The members of your remote desktop users group are always added to the local Remote Desktop Users group of every remote desktop that is joined to your domain. When adding new users, you need only add them to your remote desktop users group.

These steps apply to the Active Directory server on the domain on which VMware Horizon 8 virtual desktops or published desktops and applications are joined.

Prerequisites

Create a group for remote desktop users in your domain in Active Directory. For example, create a group named "Horizon Users".

Procedure

1. On the Active Directory server, navigate to the Group Policy Management plug-in and complete the following steps:
   a. Select **Start > Administrative Tools > Group Policy Management**.
   b. Expand your domain, right-click **Default Domain Policy**, and click **Edit**.
2. Expand the **Computer Configuration** section and open **Windows Settings\Security Settings**.
3. Right-click **Restricted Groups**, select **Add Group**, and add the Remote Desktop Users group.
4. Right-click the group and add your new remote desktop users group to the group membership list.

   For example, add "Horizon Users" to Remote Desktop Users.
5. Click **OK** to save your changes.

Using VMware Horizon 8 Group Policy Administrative Template Files

VMware Horizon 8 includes several component-specific group policy administrative (ADMX) template files.

All ADMX files that provide group policy settings for VMware Horizon 8 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 8 download, which includes the GPO Bundle containing the ZIP file.

You can optimize and secure remote desktops by adding the policy settings in these files to a new or existing GPO in Active Directory and then linking that GPO to the OU that contains your desktops.

See the *Horizon Administration* and *Horizon Remote Desktop Features and GPOs* documents for information on using VMware Horizon 8 group policy settings.

Prepare Active Directory for Smart Card Authentication

You might need to perform certain tasks in Active Directory when you implement smart card authentication.

- Add UPNs for Smart Card Users

  Because smart card logins rely on user principal names (UPNs), the Active Directory accounts of users and administrators that use smart cards to authenticate in VMware Horizon 8 must have a valid UPN.

- Add the Root Certificate to Trusted Root Certification Authorities

  If you use a certification authority (CA) to issue smart card login or domain controller certificates, you must add the root certificate to the Trusted Root Certification Authorities group policy in Active Directory. You do not need to perform this procedure if the Windows domain controller acts as the root CA.

- Add an Intermediate Certificate to Intermediate Certification Authorities

  If you use an intermediate certification authority (CA) to issue smart card login or domain controller certificates, you must add the intermediate certificate to the Intermediate Certification Authorities group policy in Active Directory.

- Add the Root Certificate to the Enterprise NTAuth Store

  If you use a CA to issue smart card login or domain controller certificates, you must add the root certificate to the Enterprise NTAuth store in Active Directory. You do not need to perform this procedure if the Windows domain controller acts as the root CA.

Add UPNs for Smart Card Users

Because smart card logins rely on user principal names (UPNs), the Active Directory accounts of users and administrators that use smart cards to authenticate in VMware Horizon 8 must have a valid UPN.

If the domain a smart card user resides in is different from the domain that your root certificate was issued from, you must set the user's UPN to the Subject Alternative Name (SAN) contained in the root certificate of the trusted CA. If your root certificate was issued from a server in the smart card user's current domain, you do not need to modify the user's UPN.

Note You might need to set the UPN for built-in Active Directory accounts, even if the certificate is issued from the same domain. Built-in accounts, including Administrator, do not have a UPN set by default.

Prerequisites

- Obtain the SAN contained in the root certificate of the trusted CA by viewing the certificate properties.

- If the ADSI Edit utility is not present on your Active Directory server, download and install the appropriate Windows Support Tools from the Microsoft Web site.

Procedure

1 On your Active Directory server, start the ADSI Edit utility.

2 In the left pane, expand the domain the user is located in and double-click `CN=Users`.

3 In the right pane, right-click the user and then click **Properties**.

4 Double-click the `userPrincipalName` attribute and type the SAN value of the trusted CA certificate.

5 Click **OK** to save the attribute setting.

Add the Root Certificate to Trusted Root Certification Authorities

If you use a certification authority (CA) to issue smart card login or domain controller certificates, you must add the root certificate to the Trusted Root Certification Authorities group policy in Active Directory. You do not need to perform this procedure if the Windows domain controller acts as the root CA.

Procedure

1 On the Active Directory server, navigate to the Group Policy Management plug-in and complete the following steps:

   a Select **Start > Administrative Tools > Group Policy Management**.

   b Expand your domain, right-click **Default Domain Policy**, and click **Edit**.

2 Expand the **Computer Configuration** section and open **Windows Settings\Security Settings\Public Key**.

3 Right-click **Trusted Root Certification Authorities** and select **Import**.

4 Follow the prompts in the wizard to import the root certificate (for example, `rootCA.cer`) and click **OK**.

5 Close the Group Policy window.

Results

All of the systems in the domain now have a copy of the root certificate in their trusted root store.

What to do next

If an intermediate certification authority (CA) issues your smart card login or domain controller certificates, add the intermediate certificate to the Intermediate Certification Authorities group policy in Active Directory. See Add an Intermediate Certificate to Intermediate Certification Authorities.

Add an Intermediate Certificate to Intermediate Certification Authorities

If you use an intermediate certification authority (CA) to issue smart card login or domain controller certificates, you must add the intermediate certificate to the Intermediate Certification Authorities group policy in Active Directory.

Procedure

1. On the Active Directory server, navigate to the Group Policy Management plug-in and complete the following steps:
   a. Select **Start > Administrative Tools > Group Policy Management**.
   b. Expand your domain, right-click **Default Domain Policy**, and click **Edit**.
2. Expand the **Computer Configuration** section and open the policy for **Windows Settings\Security Settings\Public Key**.
3. Right-click **Intermediate Certification Authorities** and select **Import**.
4. Follow the prompts in the wizard to import the intermediate certificate (for example, `intermediateCA.cer`) and click **OK**.
5. Close the Group Policy window.

Results

All of the systems in the domain now have a copy of the intermediate certificate in their intermediate certification authority store.

Add the Root Certificate to the Enterprise NTAuth Store

If you use a CA to issue smart card login or domain controller certificates, you must add the root certificate to the Enterprise NTAuth store in Active Directory. You do not need to perform this procedure if the Windows domain controller acts as the root CA.

Procedure

- On your Active Directory server, use the `certutil` command to publish the certificate to the Enterprise NTAuth store.

  For example: **`certutil -dspublish -f path_to_root_CA_cert NTAuthCA`**

Results

The CA is now trusted to issue certificates of this type.

Disable Weak Ciphers in SSL/TLS

To achieve greater security, you can configure the domain policy group policy object (GPO) to ensure that Windows-based machines running Horizon Agent do not use weak ciphers when they communicate by using the TLS protocol.

Procedure

1 To edit the GPO on the Active Directory server, select **Start > Administrative Tools > Group Policy Management**, right-click the GPO, and select **Edit**.

2 In the Group Policy Management Editor, navigate to **Computer Configuration > Policies > Administrative Templates > Network > SSL Configuration Settings**.

3 Double-click **SSL Cipher Suite Order**.

4 In the SSL Cipher Suite Order window, click **Enabled**.

5 In the Options pane, replace the entire content of the SSL Cipher Suites text box with the following cipher list:

```
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256,
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384,
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384,
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA,
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256,
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
```

The cipher suites appear on separate lines for readability. When you paste the list into the text box, the cipher suites must be on one line with no spaces after the commas.

Important In FIPS mode, list GCM cipher suites only.

Note You can amend this list of cipher suites to suit your own security policy.

6 Exit the Group Policy Management Editor.

7 To make the new group policy take effect, restart the Horizon Agent machines.

Installing Horizon Connection Server

4

To use Connection Server, you install the software on supported computers, configure the required components, and, optionally, optimize the components.

Note You can install Connection Servers in parallel if the Cloud Pod Architecture feature is not enabled on the Connection Server cluster. For more information about troubleshooting Connection Server installation errors during the parallel upgrade process, see Troubleshooting Errors During Upgrade and Installation of Connection Servers.

This chapter includes the following topics:

Installing the Horizon Connection Server Software

Depending on the performance, availability, and security needs of your VMware Horizon 8 deployment, you can install a single instance of Connection Server and replicated instances of Connection Server. You must install at least one instance of Connection Server.

When you install Connection Server, you select a type of installation.

Standard installation

Generates a Connection Server instance with a new Horizon LDAP configuration.

Replica installation

Generates a Connection Server instance with a Horizon LDAP configuration that is copied from an existing instance.

Enrollment Server installation

Installs an enrollment server that is required for the True SSO (single sign-on) feature, so that after users log in to VMware Workspace ONE Access, they can connect to a remote desktop or application without having to provide Active Directory credentials. The enrollment server requests the short-lived certificates that are used for authentication.

Note Because this feature requires that a certificate authority also be set up, and specific configuration performed, the installation procedure for the enrollment server is provided in the *Horizon Administration* document.

Installation Prerequisites for Horizon Connection Server

Before you install Connection Server, you must verify that your installation environment satisfies specific prerequisites.

- You must have a valid license for VMware Horizon 8.
- You must join the Connection Server host to an Active Directory domain. Connection Server supports certain Active Directory Domain Services (AD DS) domain functional levels. For more information, see the VMware Knowledge Base (KB) article https://kb.vmware.com/s/article/78652.

  The Connection Server host must not be a domain controller.

  Note Connection Server does not make, nor does it require, any schema or configuration updates to Active Directory.
- Do not install Connection Server on systems that have the Windows Terminal Server role installed. You must remove the Windows Terminal Server role from any system on which you install Connection Server.
- Do not install Connection Server on a system that performs any other functions or roles. For example, do not use the same system to host vCenter Server.
- The system on which you install 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.
- To run the Horizon Connection Server installer, you must use a domain user account with Administrator privileges on the system.
- When you install Connection Server, you authorize an Administrators account. You can specify the local Administrators group or a domain user or group account. VMware Horizon 8 assigns full 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 are preparing virtual machines on which to install the connection servers, you must use Sysprep on each virtual machine so that each virtual machine has a unique SID before installing Connection Server on each virtual machine separately. You can clone additional virtual machines from an existing virtual machine template but you must do so prior to installing the Connection Server on the virtual machine template. Do not install Connection Server on a virtual machine, and then clone this virtual machine that has Connection Server installed into additional Connection Server virtual machines. The correct process is to first clone a virtual machine from a virtual machine template that does not have Connection Server installed, run Sysprep on each cloned virtual machine, and then install the Connection Server on each machine separately.

Note Never import the ADAM data to a Connection Server from another Connection Server which is not part of the cluster. For example, do not import ADAM data from a different pod in a CPA environment. Doing so will override the CMS key and subsequently decryption of sensitive ADAM data will fail. This is a non recoverable error and will require building the environment again.

Install Horizon Connection Server with a New Configuration

To install Connection Server as a single server or as the first instance in a group of replicated Connection Server instances, you use the standard installation option.

When you select the standard installation option, the installation creates a new, local Horizon LDAP configuration. The installation loads the schema definitions, Directory Information Tree (DIT) definition, and ACLs and initializes the data.

After installation, you manage most Horizon LDAP configuration data by using Horizon Console . Connection Server automatically maintains some Horizon LDAP entries.

The Connection Server software cannot coexist on the same virtual or physical machine with any other VMware Horizon 8 software component, including a replica server, Horizon Agent, or Horizon Client.

When you install Connection Server with a new configuration, you can participate in a customer experience improvement program. VMware collects anonymous data about your deployment in order to improve VMware's response to user requirements. No data that identifies your organization is collected. You can choose not to participate by deselecting this option during the installation. If you change your mind about participating after the installation, you can either join or withdraw from the program by editing the Product Licensing and Usage page in Horizon Console. To review the list of fields from which data is collected, including the fields that are made anonymous, see "Information Collected by the Customer Experience Improvement Program" in the *Horizon Administration* document.

By default, the HTML Access component is installed on the Connection Server host when you install Connection Server. This component configures the VMware Horizon 8 user portal page to display an HTML Access icon in addition to the Horizon Client icon. The additional icon allows users to select HTML Access when they connect to their desktops.

For an overview of setting up Connection Server for HTML Access, see the *Horizon HTML Access Guide* document, located on the Horizon Client Documentation page.

Prerequisites

- Verify that you can log in as a domain user with administrator privileges on the Windows Server computer on which you install Connection Server.
- Verify that your installation satisfies the requirements described in Horizon Connection Server Requirements.
- Prepare your environment for the installation. See Installation Prerequisites for Horizon Connection Server.
- If you intend to authorize a domain user or group as the Administrators account, verify that you created the domain account in Active Directory.
- Prepare a data recovery password. When you back up Connection Server, the Horizon LDAP configuration is exported as encrypted LDIF data. To restore the encrypted backup VMware Horizon 8 configuration, you must provide the data recovery password. The password must contain between 1 and 128 characters. Follow your organization's best practices for generating secure passwords.

  Important You will need the data recovery password to keep VMware Horizon 8 operating and avoid downtime in a Business Continuity and Disaster Recovery (BCDR) scenario. You can provide a password reminder with the password when you install Connection Server.

- Familiarize yourself with the network ports that must be opened on the Windows Firewall for Connection Server instances. See Firewall Rules for Horizon Connection Server in VMware Horizon 8 Environments.

Procedure

1. Download the Connection Server installer file from the VMware download site at https://my.vmware.com/web/vmware/downloads.

   Under Desktop & End-User Computing, select the VMware Horizon download, which includes 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.
2. To start the Connection Server installation program, double-click the installer file.
3. Accept the VMware license terms.
4. Accept or change the destination folder.
5. Select the **Horizon Standard Server** installation option.

6 Make sure that **Install HTML Access** is selected if you intend to allow users to connect to their desktops by using a Web browser.

If **IPv4** is selected, this setting is selected by default. If **IPv6** is selected, this setting is not displayed because HTML Access is not supported in an IPv6 environment.

7 Select the Internet Protocol (IP) version, **IPv4** or **IPv6**.

You must install all VMware Horizon 8 components with the same IP version.

8 Select whether to enable or disable FIPS mode.

This option is available only if FIPS is enabled in Windows.

9 Type a data recovery password and optional password reminder.

This password is required when you recover a backup of Connection Server.

10 Choose how to configure the Windows Firewall service.

Option	Action
Configure Windows Firewall automatically	Let the installer configure Windows Firewall to allow the required network connections.
Do not configure Windows Firewall	Configure the Windows firewall rules manually. Select this option only if your organization uses its own predefined rules for configuring Windows Firewall.

11 Authorize a Horizon Administrators account.

Only members of this account can log in to Horizon Console, exercise full administration rights, and install replicated Connection Server instances and other VMware Horizon 8 servers.

Option	Description
Authorize the local Administrators group	Allows users in the local Administrators group to administer VMware Horizon 8.
Authorize a specific domain user or domain group	Allows the specified domain user or group to administer VMware Horizon 8.

12 If you specified a domain Horizon Administrators account, and you are running the installer as a local administrator or another user without access to the domain account, provide credentials to log in to the domain with an authorized user name and password.

Use *`domain name\user name`* or user principal name (UPN) format. UPN format can be *`user@domain.com`*.

13 Choose whether to participate in the customer experience improvement program.

If you participate, you can optionally select the type, size, and location of your organization.

14 Select where you want to deploy Connection Server.

Option	Description
General	If you are deploying your connection servers on-premises or in any location other those listed below. This is the default selection.
AWS	If you are deploying your connection servers on AWS or on VMware Cloud on AWS
Dell EMC	If you are deploying your connection servers on VMC on Dell EMC
Azure	If you are deploying your connection servers on Azure or on Azure VMware Solution (AVS)
Google	If you are deploying your connection servers on Google or on Google Cloud VMware Engine (GCVE)
Oracle Cloud	If you are deploying your connection servers on Oracle Cloud or on Oracle VMware Cloud Solution (OCVS)

Note This option specifies where the Connection Server is deployed. In a later step, when you add vCenter, you can specify a separate location for deploying your virtual desktops.

For example, if you want to deploy Connection Servers on native Microsoft Azure and your desktops in a VMware SDDC on the Azure VMware Solution, you would select Azure in the current step. And then when you add a vCenter, you would specify "Azure VMware Solution" as the deployment type.

15 Click **Install** to complete the wizard and install Connection Server.

16 Check for new patches on the Windows Server computer and run Windows Update as needed.

Even if you fully patched the Windows Server computer before you installed Connection Server, the installation might have enabled operating system features for the first time. Additional patches might now be required.

Results

The following VMware Horizon 8 services are installed on the Windows server computer:

- VMware Horizon Connection Server
- VMware Horizon Framework Component
- VMware Horizon Message Bus Component
- VMware Horizon Script Host
- VMware Horizon Security Gateway Component
- VMware Horizon PCoIP Secure Gateway
- VMware Horizon Blast Secure Gateway
- VMware Horizon Web Component

- VMware VDMDS, which provides Horizon LDAP services

For information about these services, see the *Horizon Administration* document.

If the **Install HTML Access** setting was selected during the installation, the HTML Access component is installed on the Windows Server computer. This component configures the HTML Access icon in the VMware Horizon user portal page and enables the **VMware Horizon Connection Server (Blast-In)** rule in the Windows Firewall. This firewall rule allows Web browsers on client devices to connect to the Connection Server on TCP port 8443.

What to do next

Configure SSL server certificates for Connection Server. See Chapter 5 Configuring TLS Certificates for VMware Horizon 8 Servers.

Perform initial configuration on Connection Server. See Chapter 6 Configuring VMware Horizon for the First Time.

If you plan to include replicated Connection Server instances in your deployment, you must install each server instance by running the Connection Server installer file.

If you are reinstalling Connection Server and you have a data collector set configured to monitor performance data, stop the data collector set and start it again.

Install Horizon Connection Server Silently

You can use the silent installation feature of the Microsoft Windows Installer (MSI) to perform a standard installation of Connection Server on several Windows computers. In a silent installation, you use the command line and do not have to respond to wizard prompts.

With silent installation, you can efficiently deploy VMware Horizon 8 components in a large enterprise.

Prerequisites

- Verify that you can log in as a domain user with administrator privileges on the Windows Server computer on which you install Connection Server.
- Verify that your installation satisfies the requirements described in Horizon Connection Server Requirements.
- Prepare your environment for the installation. See Installation Prerequisites for Horizon Connection Server.
- If you intend to authorize a domain user or group as the Horizon Administrators account, verify that you created the domain account in Active Directory.
- If you use MIT Kerberos authentication to log in to a Windows Server 2008 R2 computer on which you are installing Connection Server, install the Microsoft hotfix that is described in KB 978116 at http://support.microsoft.com/kb/978116.

- Familiarize yourself with the network ports that must be opened on the Windows Firewall for Connection Server instances. See Firewall Rules for Horizon Connection Server in VMware Horizon 8 Environments.
- Verify that the Windows computer on which you install Connection Server has version 2.0 or later of the MSI runtime engine. For details, see the Microsoft Web site.
- Familiarize yourself with the MSI installer command-line options. See Microsoft Windows Installer Command-Line Options.
- Familiarize yourself with the silent installation properties available with a standard installation of Connection Server. See Silent Installation Properties for a Horizon Connection Server Standard Installation.

Procedure

1. Download the Connection Server installer file from the VMware download site at https://my.vmware.com/web/vmware/downloads.

   Under Desktop & End-User Computing, select the VMware Horizon download, which includes 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.

2. Open a command prompt on the Windows Server computer.
3. Type the installation command on one line.

   For example: `VMware-Horizon-Connection-Server-y.y.y-xxxxxx.exe /s /v"/qn VDM_SERVER_INSTANCE_TYPE=1 VDM_INITIAL_ADMIN_SID=S-1-5-32-544 VDM_SERVER_RECOVERY_PWD=mini VDM_SERVER_RECOVERY_PWD_REMINDER=""First car"""`

   Important When you perform a silent installation, the full command line, including the data recovery password, is logged in the installer's `vminst.log` file. After the installation is complete, either delete this log file or change the data recovery password by using Horizon Console.

4. Check for new patches on the Windows Server computer and run Windows Update as needed.

   Even if you fully patched the Windows Server computer before you installed Connection Server, the installation might have enabled operating system features for the first time. Additional patches might now be required.

Results

The VMware Horizon services are installed on the Windows Server computer:

- VMware Horizon Connection Server
- VMware Horizon Framework Component

- VMware Horizon Message Bus Component
- VMware Horizon Script Host
- VMware Horizon Security Gateway Component
- VMware Horizon PCoIP Secure Gateway
- VMware Horizon Blast Secure Gateway
- VMware Horizon Web Component
- VMware VDMDS, which provides Horizon LDAP services

If the **Install HTML Access** setting was selected during the installation, the HTML Access component is installed on the Windows Server computer. This component configures the HTML Access icon in the VMware Horizon user portal page and enables the **VMware Horizon Connection Server (Blast-In)** rule in the Windows Firewall. This firewall rule allows Web browsers on client devices to connect to the Connection Server on TCP port 8443.

For information about these services, see the *Horizon Administration* document.

What to do next

Configure SSL server certificates for Connection Server. See Chapter 5 Configuring TLS Certificates for VMware Horizon 8 Servers.

If you are configuring VMware Horizon 8 for the first time, perform initial configuration on Connection Server. See Chapter 6 Configuring VMware Horizon for the First Time.

Silent Installation Properties for a Horizon Connection Server Standard Installation

You can include specific Connection Server properties when you perform a silent installation or upgrade from the command line. You must use a `PROPERTY=value` format so that Microsoft Windows Installer (MSI) can interpret the properties and values. A silent upgrade uses the same install commands.

Table 4-1. MSI Properties for Silently Installing Connection Server in a Standard Installation

MSI Property	Description	Default Value
INSTALLDIR	The path and folder in which the Connection Server software is installed. For example: `INSTALLDIR=""D:\abc\my folder""` The sets of two double quotes that enclose the path permit the MSI installer to interpret the space as a valid part of the path.	`%ProgramFiles%\VMware\VMware View\Server`
VDM_SERVER_INSTANCE_TYPE	The type of VMware Horizon 8 server installation: ■ **1**. Standard installation ■ **2**. Replica installation ■ **5**. Enrollment server installation For example, to perform a standard installation, define `VDM_SERVER_INSTANCE_TYPE=1`	1

Table 4-1. MSI Properties for Silently Installing Connection Server in a Standard Installation (continued)

MSI Property	Description	Default Value
HTMLACCESS	Controls the HTML Access add-on installation. Set this property to 1 to configure HTML Access or omit the property if HTML Access is not needed.	1
VDM_IP_PROTOCOL_USAGE	Specifies the IP version that VMware Horizon 8 components use for communication. The possible values are **IPv4** and **IPv6**.	**IPv4**
VDM_SERVER_RECOVERY_PWD	The data recovery password. If a data recovery password is not set in Horizon LDAP, this property is mandatory. The password must contain between 1 and 128 characters. Follow your organization's best practices for generating secure passwords.	None
VDM_SERVER_RECOVERY_PWD_REMINDER	The data recovery password reminder. This property is optional.	None
FWCHOICE	The MSI property that determines whether to configure a firewall for the Connection Server instance. A value of 1 configures a firewall. A value of 2 does not configure a firewall. For example: `FWCHOICE=1`	1
VDM_INITIAL_ADMIN_SID	The SID of the initial Horizon Administrators user or group that is authorized with full administration rights in VMware Horizon 8. The default value is the SID of the local Administrators group on the Connection Server computer. You can specify a SID of a domain user or group account.	`S-1-5-32-544`
DEPLOYMENT_TYPE	Provide the location where you will deploy Connection Server. If you do not provide a deployment type, the default is an on-premises installation. For a list of deployment types, see Install Horizon Connection Server with a New Configuration.	GENERAL
VDM_FIPS_ENABLED	Specifies whether to enable or disable FIPS mode. A value of 1 enables FIPS mode. A value of 0 disables FIPS mode. If this property is set to 1 and Windows is not in FIPS mode, the installer will abort.	0

Install a Replicated Instance of Horizon Connection Server

To provide high availability and load balancing, you can install one or more additional instances of Connection Server that replicate an existing Connection Server instance. After a replica installation, the existing and newly installed instances of Connection Server are identical.

When you install a replicated instance, VMware Horizon 8copies the Horizon LDAP configuration data from the existing Connection Server instance.

After the installation, identical Horizon LDAP configuration data is maintained on all Connection Server instances in the replicated group. When a change is made on one instance, the updated information is copied to the other instances.

If a replicated instance fails, the other instances in the group continue to operate. When the failed instance resumes activity, its configuration is updated with the changes that took place during the outage.

Note Replication functionality is provided by Horizon LDAP, which uses the same replication technology as Active Directory.

The replica server software cannot coexist on the same virtual or physical machine with any other VMware Horizon 8 software component, including a Connection Server, Horizon Agent, or Horizon Client.

By default, the HTML Access component is installed on the Connection Server host when you install Connection Server. This component configures the VMware Horizon 8 user portal page to display an HTML Access icon in addition to the Horizon Client icon. The additional icon allows users to select HTML Access when they connect to their desktops.

For an overview of setting up Connection Server for HTML Access, see the *Horizon HTML Access Guide* document, located on the Horizon Client Documentation page.

Prerequisites

- Verify that at least one Connection Server instance is installed and configured on the network.
- To install the replicated instance, you must log in as a user with the Administrators role. You specify the account or group with the Administrators role when you install the first instance of Connection Server. The role can be assigned to the local Administrators group or a domain user or group. See Install Horizon Connection Server with a New Configuration.
- If the existing Connection Server instance is in a different domain than the replicated instance, the domain user must also have Administrator privileges on the Windows Server computer where the existing instance is installed.
- Verify that your installation satisfies the requirements described in Horizon Connection Server Requirements.
- Verify that the computers on which you install replicated Connection Server instances are connected over a high-performance LAN. See Network Requirements for Replicated Horizon Connection Server Instances - Install Only.
- Prepare your environment for the installation. See Installation Prerequisites for Horizon Connection Server.
- Prepare a data recovery password. See Install Horizon Connection Server with a New Configuration.

- Familiarize yourself with the network ports that must be opened on the Windows Firewall for Connection Server instances. See Firewall Rules for Horizon Connection Server in VMware Horizon 8 Environments.

Procedure

1 Download the Connection Server installer file from the VMware download site at https://my.vmware.com/web/vmware/downloads.

Under Desktop & End-User Computing, select the VMware Horizon download, which includes 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.

2 To start the Connection Server installation program, double-click the installer file.

3 Accept the VMware license terms.

4 Accept or change the destination folder.

5 Select the **Horizon Replica Server** installation option.

6 Select the Internet Protocol (IP) version, **IPv4** or **IPv6**.

You must install all VMware Horizon 8 components with the same IP version.

7 Select whether to enable or disable FIPS mode.

This option is available only if FIPS mode is enabled in Windows.

8 Make sure that **Install HTML Access** is selected if you intend to allow users to connect to their desktops by using HTML Access.

If **IPv4** is selected, this setting is selected by default. If **IPv6** is selected, this setting is not displayed because HTML Access is not supported in an IPv6 environment.

9 Enter the host name or IP address of the existing Connection Server instance you are replicating.

10 Type a data recovery password and, optionally, a password reminder.

11 Choose how to configure the Windows Firewall service.

Option	Action
Configure Windows Firewall automatically	Let the installer configure Windows Firewall to allow the required network connections.
Do not configure Windows Firewall	Configure the Windows firewall rules manually. Select this option only if your organization uses its own predefined rules for configuring Windows Firewall.

12 Complete the installation wizard to finish installing the replicated instance.

13 Check for new patches on the Windows Server computer and run Windows Update as needed.

   Even if you fully patched the Windows Server computer before you installed Connection Server, the installation might have enabled operating system features for the first time. Additional patches might now be required.

Results

The VMware Horizon services are installed on the Windows Server computer:

- VMware Horizon Connection Server
- VMware Horizon Framework Component
- VMware Horizon Message Bus Component
- VMware Horizon Script Host
- VMware Horizon Security Gateway Component
- VMware Horizon PCoIP Secure Gateway
- VMware Horizon Blast Secure Gateway
- VMware Horizon Web Component
- VMware VDMDS, which provides Horizon LDAP services

For information about these services, see the *Horizon Administration* document.

If the **Install HTML Access** setting was selected during the installation, the HTML Access component is installed on the Windows Server computer. This component configures the HTML Access icon in the VMware Horizon user portal page and enables the **VMware Horizon Connection Server (Blast-In)** rule in the Windows Firewall. This firewall rule allows Web browsers on client devices to connect to the Connection Server on TCP port 8443.

What to do next

Configure an SSL server certificate for the Connection Server instance. See Chapter 5 Configuring TLS Certificates for VMware Horizon 8 Servers.

You do not have to perform an initial VMware Horizon 8 configuration on a replicated instance of Connection Server. The replicated instance inherits its configuration from the existing Connection Server instance.

However, you might have to configure client connection settings for this Connection Server instance, and you can tune Windows Server settings to support a large deployment. See Configuring Horizon Client Connections and Sizing Windows Server Settings to Support Your Deployment.

If you are reinstalling Connection Server and you have a data collector set configured to monitor performance data, stop the data collector set and start it again.

Install a Replicated Instance of Horizon Connection Server Silently

You can use the silent installation feature of the Microsoft Windows Installer (MSI) to install a replicated instance of Connection Server on several Windows computers. In a silent installation, you use the command line and do not have to respond to wizard prompts.

With silent installation, you can efficiently deploy VMware Horizon 8 components in a large enterprise.

Prerequisites

- Verify that at least one Connection Server instance is installed and configured on the network.
- To install the replicated instance, you must log in as a user with credentials to access the Administrators account. You specify the Administrators account when you install the first instance of Connection Server. The account can be the local Administrators group or a domain user or group account. See Install Horizon Connection Server with a New Configuration.
- If the existing Connection Server instance is in a different domain than the replicated instance, the domain user must also have Administrator privileges on the Windows Server computer where the existing instance is installed.
- Verify that your installation satisfies the requirements described in Horizon Connection Server Requirements.
- Verify that the computers on which you install replicated Connection Server instances are connected over a high-performance LAN. See Network Requirements for Replicated Horizon Connection Server Instances - Install Only.
- Prepare your environment for the installation. See Installation Prerequisites for Horizon Connection Server.
- Familiarize yourself with the network ports that must be opened on the Windows Firewall for Connection Server instances. See Firewall Rules for Horizon Connection Server in VMware Horizon 8 Environments.
- Familiarize yourself with the MSI installer command-line options. See Microsoft Windows Installer Command-Line Options.
- Familiarize yourself with the silent installation properties available with a replica installation of Connection Server. See Silent Installation Properties for a Replicated Instance of Horizon Connection Server.

Procedure

1 Download the Connection Server installer file from the VMware download site at https://my.vmware.com/web/vmware/downloads.

  Under Desktop & End-User Computing, select the VMware Horizon download, which includes 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.

2 Open a command prompt on the Windows Server computer.

3 Type the installation command on one line.

For example: `VMware-Horizon-Connection-Server-y.y.y-xxxxxx.exe /s /v"/qn VDM_SERVER_INSTANCE_TYPE=2 ADAM_PRIMARY_NAME=cs1.companydomain.com VDM_INITIAL_ADMIN_SID=S-1-5-32-544"`

If you install a replicated Connection Server instance that is View 5.1 or later, and the existing Connection Server instance you are replicating is View 5.0.*x* or earlier, you must specify a data recovery password, and you can add a password reminder. For example: `VMware-Horizon-Connection-Server-y.y.y-xxxxxx.exe /s /v"/qn VDM_SERVER_INSTANCE_TYPE=2 ADAM_PRIMARY_NAME=cs1.companydomain.com VDM_INITIAL_ADMIN_SID=S-1-5-32-544 VDM_SERVER_RECOVERY_PWD=mini VDM_SERVER_RECOVERY_PWD_REMINDER=""First car"""`

Important When you perform a silent installation, the full command line, including the data recovery password, is logged in the installer's `vminst.log` file. After the installation is complete, either delete this log file or change the data recovery password by using Horizon Console.

4 Check for new patches on the Windows Server computer and run Windows Update as needed.

Even if you fully patched the Windows Server computer before you installed Connection Server, the installation might have enabled operating system features for the first time. Additional patches might now be required.

Results

The VMware Horizon services are installed on the Windows Server computer:

- VMware Horizon Connection Server
- VMware Horizon Framework Component
- VMware Horizon Message Bus Component
- VMware Horizon Script Host
- VMware Horizon Security Gateway Component
- VMware Horizon PCoIP Secure Gateway
- VMware Horizon Blast Secure Gateway
- VMware Horizon Web Component
- VMware VDMDS, which provides Horizon LDAP services

For information about these services, see the *Horizon Administration* document.

If the **Install HTML Access** setting was selected during the installation, the HTML Access component is installed on the Windows Server computer. This component configures the HTML Access icon in the VMware Horizon user portal page and enables the **VMware Horizon Connection Server (Blast-In)** rule in the Windows Firewall. This firewall rule allows Web browsers on client devices to connect to the Connection Server on TCP port 8443.

What to do next

Configure an SSL server certificate for the Connection Server instance. See Chapter 5 Configuring TLS Certificates for VMware Horizon 8 Servers.

You do not have to perform an initial VMware Horizon 8 configuration on a replicated instance of Connection Server. The replicated instance inherits its configuration from the existing Connection Server instance.

However, you might have to configure client connection settings for this Connection Server instance, and you can tune Windows Server settings to support a large deployment. See Configuring Horizon Client Connections and Sizing Windows Server Settings to Support Your Deployment.

Silent Installation Properties for a Replicated Instance of Horizon Connection Server

You can include specific properties when you silently install a replicated Horizon Connection Server instance from the command line. You must use a `PROPERTY=value` format so that Microsoft Windows Installer (MSI) can interpret the properties and values.

Table 4-2. MSI Properties for Silently installing a Replicated Instance of Horizon Connection Server

MSI Property	Description	Default Value
INSTALLDIR	The path and folder in which the Connection Server software is installed. For example: `INSTALLDIR=""D:\abc\my folder""` The sets of two double quotes that enclose the path permit the MSI installer to interpret the space as a valid part of the path. This MSI property is optional.	`%ProgramFiles%\VMware\VMware View\Server`
VDM_SERVER_INSTANCE_TYPE	The type of Connection Server installation: ■ 1. Standard installation ■ 2. Replica installation To install a replicated instance, define `VDM_SERVER_INSTANCE_TYPE=2` This MSI property is required when installing a replica.	1
ADAM_PRIMARY_NAME	The host name or IP address of the existing Connection Server instance you are replicating. For example: `ADAM_PRIMARY_NAME=cs1.companydomain.com` This MSI property is required.	None

Table 4-2. MSI Properties for Silently installing a Replicated Instance of Horizon Connection Server (continued)

MSI Property	Description	Default Value
FWCHOICE	The MSI property that determines whether to configure a firewall for the Connection Server instance. A value of 1 configures a firewall. A value of 2 does not configure a firewall. For example: `FWCHOICE=1` This MSI property is optional.	1
VDM_SERVER_ RECOVERY_PWD	The data recovery password. If a data recovery password is not set in Horizon LDAP, this property is mandatory. The password must contain between 1 and 128 characters. Follow your organization's best practices for generating secure passwords.	None
VDM_SERVER_RECOVERY_ PWD_REMINDER	The data recovery password reminder. This property is optional.	None
VDM_IP_PROTOCOL_ USAGE	Specifies the IP version that VMware Horizon components use for communication. The possible values are **`IPv4`** and **`IPv6`**	**`IPv4`**
VDM_FIPS_ENABLED	Specifies whether to enable or disable FIPS mode. A value of 1 enables FIPS mode. A value of 0 disables FIPS mode. If this property is set to 1 and Windows is not in FIPS mode, the installer will abort.	0

Unified Access Gateway Appliance Advantages over VPN

A Unified Access Gateway appliance is a default gateway for secure access to remote desktops and applications from outside the corporate firewall.

For the latest version of Unified Access Gateway documentation, see the *Deploying and Configuring VMware Unified Access Gateway* document in https://docs.vmware.com/en/Unified-Access-Gateway/index.html.

A Unified Access Gateway appliance resides within a network demilitarized zone (DMZ) and acts as a proxy host for connections inside a trusted network, providing an additional layer of security by shielding virtual desktops, application hosts, and servers from the public-facing Internet.

Configure a Unified Access Gateway Appliance

Unified Access Gateway and generic VPN solutions are similar as they both ensure that traffic is forwarded to an internal network only on behalf of strongly authenticated users.

Unified Access Gateway advantages over generic VPN include the following.

- Access Control Manager. Unified Access Gateway applies access rules automatically. Unified Access Gateway recognizes the entitlements of the users and the addressing required to connect internally. A VPN does the same, because most VPNs allow an administrator to configure network connection rules for every user or group of users individually. At first, this works well with a VPN, but requires significant administrative effort to maintain the required rules.
- User Interface. Unified Access Gateway does not alter the straightforward Horizon Client user interface. With Unified Access Gateway, when the Horizon Client is launched, authenticated users are in their View environment and have controlled access to their desktops and applications. A VPN requires that you must set up the VPN software first and authenticate separately before starting the Horizon Client.
- Performance. Unified Access Gateway is designed to maximize security and performance. With Unified Access Gateway, PCoIP, HTML access, and WebSocket protocols are secured without requiring additional encapsulation. VPNs are implemented as SSL VPNs. This implementation meets security requirements and, with Transport Layer Security (TLS) enabled, is considered secure, but the underlying protocol with SSL/TLS is just TCP-based. With modern video remoting protocols exploiting connectionless UDP-based transports, the performance benefits can be significantly eroded when forced over a TCP-based transport. This does not apply to all VPN technologies, as those that can also operate with DTLS or IPsec instead of SSL/TLS can work well with VMware Horizon 8 desktop protocols.

Enhance VMware Horizon 8 Security with Unified Access Gateway

A Unified Access Gateway appliance enhances security by layering device certification authentication on top of user authentication so access can be restricted only from known good devices and adding another layer of security on virtual desktop infrastructure.

Note This feature is supported in Horizon Client for Windows only.

- See Configuring Certificate or Smart Card Authentication on the Unified Access Gateway appliance in the *Deploying and Configuring VMware Unified Access Gateway* document in https://docs.vmware.com/en/Unified-Access-Gateway/index.html.
- The Endpoint Compliance Checks feature provides an extra layer of security for accessing desktops in addition to the other user authentication services that are available on Unified Access Gateway. See Endpoint Compliance Checks for Horizon in the *Deploying and Configuring VMware Unified Access Gateway* document in https://docs.vmware.com/en/Unified-Access-Gateway/index.html.

Important When a Unified Access Gateway appliance is configured for two-factor authentication (RSA SecureID and RADIUS) and Windows user name matching is enabled, and there are multiple user domains, you should enable Connection Server to send the domain list so that the user can select the correct domain while using the Windows username and password for authentication.

Double-hop DMZ

For cases where a double-hop DMZ between the Internet and the internal network is required, you can deploy a Unified Access Gateway appliance in the outer DMZ as a Web Reverse Proxy with Unified Access Gateway in the inner DMZ to create a double-hop DMZ configuration. Traffic passes through a specific reverse proxy in each DMZ layer and cannot bypass a DMZ layer.
For configuration details, see the *Deploying and Configuring VMware Unified Access Gateway* document.

Horizon LDAP

Horizon LDAP is the data repository for all VMware Horizon 8 configuration information. Horizon LDAP is an embedded Lightweight Directory Access Protocol (LDAP) directory that is provided with the Connection Server installation

Horizon LDAP contains standard LDAP directory components that are used by VMware Horizon 8.

- VMware Horizon 8 schema definitions
- Directory information tree (DIT) definitions
- Access control lists (ACLs)

Horizon LDAP contains directory entries that represent VMware Horizon 8 objects.

- Remote desktop entries that represent each accessible desktop. Each entry contains references to the Foreign Security Principal (FSP) entries of Windows users and groups in Active Directory who are authorized to use the desktop.
- Remote desktop pool entries that represent multiple desktops managed together
- Virtual machine entries that represent the vCenter Server virtual machine for each remote desktop
- VMware Horizon 8 component entries that store configuration settings

Horizon LDAP also contains a set of VMware Horizon 8 plug-in DLLs that provide automation and notification services for other VMware Horizon 8 components.

LDAP Replication

When you install a replicated instance of Connection Server, VMware Horizon 8 copies the Horizon LDAP configuration data from the existing Connection Server instance. Identical Horizon LDAP configuration data is maintained on all Connection Server instances in the replicated group. When a change is made on one instance, the updated information is copied to the other instances.

If a replicated instance fails, the other instances in the group continue to operate. When the failed instance resumes activity, its configuration is updated with the changes that took place during the outage. With VMware Horizon 8 and later releases, a replication status check is performed every 15 minutes to determine whether each instance can communicate with the other servers in the replicated group and whether each instance can fetch LDAP updates from the other servers in the group.

You can use the dashboard in Horizon Console to check the replication status. If any Connection Server instances have a red icon in the dashboard, click the icon to see 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 VDMDS DSA options might be blocking the replications
- A network problem has occurred

By default, the replication check occurs every 15 minutes. You can use ADSI Edit on a Connection Server instance to change the interval. To set the number of minutes, connect to **DC=vdi,DC=vmware,DC=int** and edit the **pae-ReplicationStatusDataExpiryInMins** attribute on the **CN=Common,OU=Global,OU=Properties** object.

The **pae-ReplicationStatusDataExpiryInMins** attribute value should be between 10 minutes and 1440 minutes (one day). If the attribute value is less than 10 minutes, VMware Horizon 8 treats it as 10 minutes. If the attribute value is greater than 1440, VMware Horizon 8 treats it as 1440 minutes.

Firewall Rules for Horizon Connection Server in VMware Horizon 8 Environments

Certain ports must be opened on the firewall for Connection Server instances.

When you install Connection Server, the installation application can optionally configure the required Windows Firewall rules for you. These rules open the ports that are used by default. If you change the default ports after installation, you must manually configure Windows Firewall to allow Horizon Client devices to connect to VMware Horizon 8 through the updated ports.

The following table lists the default ports that can be opened automatically during installation. Ports are incoming unless otherwise noted.

Table 4-3. Ports Opened During Horizon Connection Server Installation

Protocol	Ports	Horizon Connection Server Instance Type
JMS	TCP 4001	Standard and replica
JMS	TCP 4002	Standard and replica
JMSIR	TCP 4100	Standard and replica
JMSIR	TCP 4101	Standard and replica
AJP13	TCP 8009	Standard and replica
HTTP	TCP 80	Standard, replica
HTTPS	TCP 443	Standard, replica

Table 4-3. Ports Opened During Horizon Connection Server Installation (continued)

Protocol	Ports	Horizon Connection Server Instance Type
PCoIP	TCP 4172 in; UDP 4172 both directions	Standard, replica
HTTPS	TCP 8443 UDP 8443	Standard, replica After the initial connection to VMware Horizon 8 is made, the Web browser or client device connects to the Blast Secure Gateway on TCP port 8443. The Blast Secure Gateway must be enabled on a Connection Server instance to allow this second connection to take place.
HTTPS	TCP 8472	Standard and replica For the Cloud Pod Architecture feature: used for inter-pod communication.
HTTP	TCP 22389	Standard and replica For the Cloud Pod Architecture feature: used for global LDAP replication.
HTTPS	TCP 22636	Standard and replica For the Cloud Pod Architecture feature: used for secure global LDAP replication.

Reinstall Horizon Connection Server with a Backup Configuration

In certain situations, you might have to reinstall the current version of a Connection Server instance and restore the existing VMware Horizon 8 configuration by importing a backup LDIF file that contains the Horizon LDAP configuration data.

For example, as part of a business continuity and disaster recovery (BC/DR) plan, you might want to have a procedure ready to implement in case a datacenter stops functioning. The first step in such a plan is to ensure that the Horizon LDAP configuration is backed up in another location. A second step is to install Connection Server in the new location and import the backup configuration, as described in this procedure.

You might also use this procedure when you set up a second datacenter with the existing VMware Horizon 8 configuration. Or you might use it if your VMware Horizon 8 deployment contains only a single Connection Server instance, and a problem occurs with that server.

You do not have to follow this procedure if you have multiple Connection Server instances in a replicated group, and a single instance goes down. You can simply reinstall Connection Server as a replicated instance. During the installation, you provide connection information to another Connection Server instance, and VMware Horizon 8 restores the Horizon LDAP configuration from the other instance.

Prerequisites

- Verify that the Horizon LDAP configuration was backed up to an encrypted LDIF file.
- Familiarize yourself with restoring a Horizon LDAP configuration from an LDIF backup file by using the `vdmimport` command.

See "Backing Up and Restoring VMware Horizon 8 Configuration Data" in the *Horizon Administration* document.

- Familiarize yourself with the steps for installing a new Connection Server instance. See Install Horizon Connection Server with a New Configuration.

Procedure

1. Install Connection Server with a new configuration.
2. Decrypt the encrypted LDIF file.

   For example:

   ```
   vdmimport -d -p mypassword
   -f MyEncryptedexport.LDF > MyDecryptedexport.LDF
   ```

3. Import the decrypted LDIF file to restore the Horizon LDAP configuration.

   For example:

   ```
   vdmimport -f MyDecryptedexport.LDF
   ```

   Note At this stage, the VMware Horizon 8 configuration is not yet accessible. Clients cannot access Connection Server or connect to their desktops.

4. Uninstall the Connection Server from the computer by using the Windows **Add/Remove Programs** utility.

   Do not uninstall the Horizon LDAP configuration, called the AD LDS Instance VMwareVDMDS instance. You can use the **Add/Remove Programs** utility to verify that the AD LDS Instance VMwareVDMDS instance was not removed from the Windows Server computer.

5. Reinstall Connection Server.

   At the installer prompt, accept the existing Horizon LDAP.

What to do next

Configure Connection Server and your VMware Horizon 8 environment as you would after you install a Connection Server instance with a new configuration.

Microsoft Windows Installer Command-Line Options

To install VMware Horizon 8 components silently, you must use Microsoft Windows Installer (MSI) command-line options and properties. The Horizon 8 component installers are MSI programs and use standard MSI features.

For details about MSI, see the Microsoft Web site. For MSI command-line options, see the Microsoft Developer Network (MSDN) Library Web site and search for MSI command-line options. To see MSI command-line usage, you can open a command prompt on the Horizon 8 component computer and type `msiexec /?`.

To run a Horizon 8 component installer silently, you begin by silencing the bootstrap program that extracts the installer into a temporary directory and starts an interactive installation.

At the command line, you must enter command-line options that control the installer's bootstrap program.

Table 4-4. Command-Line Options for a Horizon 8 Component's Bootstrap Program

Option	Description
`/s`	Disables the bootstrap splash screen and extraction dialog, which prevents the display of interactive dialogs. For example: `VMware-Horizon-Connection-Server-y.y.y-xxxxxx.exe /s` The `/s` option is required to run a silent installation.
`/v" MSI_command_line_options"`	Instructs the installer to pass the double-quote-enclosed string that you enter at the command line as a set of options for MSI to interpret. You must enclose your command-line entries between double quotes. Place a double quote after the `/v` and at the end of the command line. For example: `VMware-Horizon-Agent-x86-YYMM-y.y.y-xxxxxx.exe /s /v"command_line_options"` To instruct the MSI installer to interpret a string that contains spaces, enclose the string in two sets of double quotes. For example, you might want to install the Horizon 8 component in an installation path name that contains spaces. For example: `VMware-Horizon-Connection-Server-y.y.y-xxxxxx.exe /s /v"command_line_options INSTALLDIR=""d:\abc\my folder"""` In this example, the MSI installer passes on the installation-directory path and does not attempt to interpret the string as two command-line options. Note the final double quote that encloses the entire command line. The `/v"command_line_options"` option is required to run a silent installation.

You control the remainder of a silent installation by passing command-line options and MSI property values to the MSI installer, `msiexec.exe`. The MSI installer includes the Horizon 8 component's installation code. The installer uses the values and options that you enter in the command line to interpret installation choices and setup options that are specific to the Horizon 8 component.

Table 4-5. MSI Command-Line Options and MSI Properties

MSI Option or Property	Description
/qn	Instructs the MSI installer not to display the installer wizard pages. For example, you might want to install Horizon Agent silently and use only default setup options and features: VMware-Horizon-Agent-x86-YYMM-y.y.y-xxxxxx.exe /s /v"/qn" Alternatively, you can use the /qb option to display a basic progress dialog box in a noninteractive, automated installation. The /qn or /qb option is required to run a silent installation. For information about additional /q parameters, see the Microsoft Dev Center website.
INSTALLDIR	Specifies an alternative installation path for the Horizon 8 component. Use the format *INSTALLDIR=path* to specify an installation path. You can ignore this MSI property if you want to install the Horizon 8 component in the default path. This MSI property is optional.
ADDLOCAL	Determines the component-specific options to install. In an interactive installation, the Horizon 8 installer displays custom setup options that you can select or deselect. In a silent installation, you can use the ADDLOCAL property to selectively install individual setup options by specifying the options on the command line. Options that you do not explicitly specify are not installed. In both interactive and silent installations, the Horizon 8 installer automatically installs certain features. You cannot use ADDLOCAL to control whether or not to install these non-optional features. Type ADDLOCAL=ALL to install all custom setup options that can be installed during an interactive installation, including those that are installed by default and those that you must select to install, except NGVC. NGVC and SVIAgent are mutually exclusive. The following example installs Core, BlastProtocol, PCoIP, UnityTouch, VmVideo, PSG, and all features that are supported on the guest operating system: VMware-Horizon-Agent-x86-YYMM-y.y.y-xxxxxx.exe /s /v"/qn ADDLOCAL=ALL" If you do not use the ADDLOCAL property, the custom setup options that are installed by default and the automatically installed features are installed. Custom setup options that are off (unselected) by default are not installed. The following example installs Core, BlastProtocol, PCoIP, UnityTouch, VmVideo, PSG, and the on-by-default custom setup options that are supported on the guest operating system: VMware-Horizon-Agent-x86-YYMM-y.y.y-xxxxxx.exe /s /v"/qn" To specify individual setup options, type a comma-separated list of setup option names. Do not use spaces between names. Use the format ADDLOCAL=*value,value,value...*. You must include Core when you use the ADDLOCAL=*value,value,value...* property. The following example installs Horizon Agent with the Core, BlastProtocol, PCoIP, UnityTouch, VmVideo, PSG, and Instant Clone Agent features: VMware-Horizon-Agent-x86-YYMM-y.y.y-xxxxxx.exe /s /v"/qn ADDLOCAL=Core,NGVC The preceding example does not install other components, even those that are installed by default interactively. The ADDLOCAL MSI property is optional.
REBOOT	You can use the REBOOT=ReallySuppress option to allow system configuration tasks to complete before the system reboots. This MSI property is optional.

Table 4-5. MSI Command-Line Options and MSI Properties (continued)

MSI Option or Property	Description
`REINSTALL`	You can use the `REINSTALL=ALL` option to install a Horizon Agent patch. The following example installs the patch: `msiexec /p VMware-Horizon-Agent-x86_64-YYMM-y.y.y-xxxxxx.msp /qn REINSTALL=ALL` This MSI property is optional.
`REMOVE`	You can use the `REMOVE=<value>` option to remove a feature. The following example uninstalls the USB feature: `VMware-Horizon-Agent-x86-YYMM-y.y.y-xxxxxx.exe /s /v"/qn REMOVE=USB"` This MSI property is optional.
`/l*v` *log_file*	Writes logging information into the specified log file with verbose output. For example: `/l*v ""%TEMP%\vmmsi.log""` This example generates a detailed log file that is similar to the log generated during an interactive installation. You can use this option to record custom features that might apply uniquely to your installation. You can use the recorded information to specify installation features in future silent installations. The `/l*v` option is optional.

Uninstalling VMware Horizon 8 Components Silently by Using MSI Command-Line Options

You can uninstall VMware Horizon 8 components by using Microsoft Windows Installer (MSI) command-line options.

Syntax

```
msiexec.exe
/qb
/x
product_code
```

Options

The `/qb` option displays the uninstall progress bar. To suppress displaying the uninstall progress bar, replace the `/qb` option with the `/qn` option.

The `/x` option uninstalls the VMware Horizon 8 component.

The *product_code* string identifies the VMware Horizon 8 component product files to the MSI uninstaller. You can find the *product_code* string by searching for `ProductCode` in the `%TEMP%\vmmsi.log` file that is created during the installation. To find the *product_code* string that applies to older versions of VMware Horizon 8 components, see the VMware Knowledge Base (KB) article at http://kb.vmware.com/kb/2064845.

For information about MSI command-line options, see Microsoft Windows Installer Command-Line Options.

Uninstall a Horizon Agent Example

To uninstall a 32-bit Horizon Agent, enter the following command:

```
msiexec.exe /qb /x {B23352D8-AD44-4379-A56E-0E337F9C4036}
```

To uninstall a 64-bit Horizon Agent, enter the following command:

```
msiexec.exe /qb /x {53D6EE37-6B10-4963-81B1-8E2972A1DA4D}
```

Add a verbose log to the command.

```
/l*v "%TEMP%\vmmsi_uninstall.log"
```

If you do not explicitly pass the `/l` option, the default verbose log file is `%TEMP%\MSI`*nnnn*`.log`, where *nnnn* is a four-character GUID.

The Horizon Agent uninstallation process retains some registry keys. These keys are required for retaining the Connection Server configuration information that enables the remote desktop to continue being paired with the Connection Server even if the agent is uninstalled and then reinstalled. Removing these registry keys will break that pairing.

The following registry keys are retained:

- `HKLM\SOFTWARE\Microsoft\SystemCertificates\VMware Horizon View Certificates\*`
- `HKLM\SOFTWARE\Microsoft\SystemCertificates\VMwareView\Certificates\*`
- `HKLM\SOFTWARE\Microsoft\SystemCertificates\VMwareView\CRLs`
- `HKLM\SOFTWARE\Microsoft\SystemCertificates\VMwareView\CTLs`
- `HKLM\SOFTWARE\Policies\VMware, Inc.\VMware VDM\*`
- `HKLM\SOFTWARE\Policies\VMware, Inc.\Horizon Monitoring Service Agent\*`
- `HKLM\SOFTWARE\VMware, Inc.\VMware VDM\*`
- `HKLM\SOFTWARE\Wow6432Node\Microsoft\SystemCertificates\VMware Horizon View Certificates\*`
- `HKLM\SOFTWARE\Wow6432Node\Microsoft\SystemCertificates\VMwareView\*`
- `HKLM\SOFTWARE\Wow6432Node\Policies\VMware, Inc.\VMware VDM\*`

- HKLM\SOFTWARE\Wow6432Node\Policies\VMware, Inc.\Horizon Monitoring Service Agent*
- HKLM\SOFTWARE\Wow6432Node\VMware, Inc.
- HKLM\SOFTWARE\Wow6432Node\VMware, Inc.\VMware VDM

Configuring TLS Certificates for VMware Horizon 8 Servers

5

VMware strongly recommends that you configure TLS certificates for authentication of Connection Server instances.

A default TLS server certificate is generated when you install Connection Server instances. You can use the default certificate for testing purposes.

Certificates used for communication between Connection Servers and also between Horizon Agents and Connection Server instances, are replaced using an automatic mechanism, and cannot be replaced manually. For more details, see the *Horizon Security* document.

Important Replace the default certificate as soon as possible. The default certificate is not signed by a Certificate Authority (CA). Use of certificates that are not signed by a CA can allow untrusted parties to intercept traffic by masquerading as your server.

This chapter includes the following topics:

- Troubleshooting Certificate Issues on Horizon Connection Server

Understanding TLS Certificates for VMware Horizon 8 Servers

You must follow certain guidelines for configuring TLS certificates for VMware Horizon 8 servers and related components.

Horizon Connection Server

TLS is required for client connections to a server. Client-facing Connection Server instances and intermediate servers that terminate TLS connections require TLS server certificates.

By default, when you install Connection Server, the installation generates a self-signed certificate for the server. However, the installation uses an existing certificate in the following cases:

- If a valid certificate with a Friendly name of `vdm` already exists in the Windows Certificate Store
- If you upgrade to VMware Horizon 8 from an earlier release, and a valid keystore file is configured on the Windows Server computer, the installation extracts the keys and certificates and imports them into the Windows Certificate Store.

vCenter Server

Before you add vCenter Server to VMware Horizon 8 in a production environment, make sure that vCenter Server uses certificates that are signed by a CA.

For information about replacing the default certificate for vCenter Server, see "Certificate Replacement in Large Deployments" in the *vSphere Authentication* document on the VMware vSphere Documentation site.

PCoIP Secure Gateway

To comply with industry or jurisdiction security regulations, you can replace the default TLS certificate that is generated by the PCoIP Secure Gateway (PSG) service with a certificate that is signed by a CA. Configuring the PSG service to use a CA-signed certificate is highly recommended, particularly for deployments that require you to use security scanners to pass compliance testing. See Configure the PCoIP Secure Gateway to Use a New TLS Certificate.

Blast Secure Gateway

By default, the Blast Secure Gateway (BSG) uses the TLS certificate that is configured for the Connection Server instance on which the BSG is running. If you replace the default, self-signed certificate for a server with a CA-signed certificate, the BSG also uses the CA-signed certificate.

Enrollment Server

TLS is required for connections to an enrollment server from Connection Server. By default, Enrollment Server generates a self-signed certificate for the server. However, the installation uses an existing certificate if a valid certificate with a Friendly name of **vdm.es** already exists in the Windows Certificate Store.

Database Server

To enable TLS for communication with a Database server used to host Event DB, make sure that the Database server uses a certificate signed by a CA. Refer to documentation from the respective database provider to set up the TLS certificate on the database servers.

SAML 2.0 Authenticator

VMware Workspace ONE Access uses SAML 2.0 authenticators to provide Web-based authentication and authorization across security domains. If you want VMware Horizon 8 to delegate authentication to VMware Workspace ONE Access, you can configure VMware Horizon 8 to accept SAML 2.0 authenticated sessions from VMware Workspace ONE Access. When VMware Workspace ONE Access is configured to support VMware Horizon 8, VMware Workspace ONE Access users can connect to remote desktops by selecting desktop icons on the Horizon User Portal.

In Horizon Console, you can configure SAML 2.0 authenticators for use with Connection Server instances.

Before you add a SAML 2.0 authenticator in Horizon Console, make sure that the SAML 2.0 authenticator uses a certificate that is signed by a CA.

Additional Guidelines

For general information about requesting and using TLS certificates that are signed by a CA, see Benefits of Using TLS Certificates Signed by a CA.

When client endpoints connect to a Connection Server instance, they are presented with the server's TLS server certificate and any intermediate certificates in the trust chain (intermediate certificates are in the Connection Server's Windows Intermediate Certification Authorities store). To trust the server certificate, the client systems must have installed the root certificate of the signing CA.

vCenter Server does not present an intermediate certificate while making a TLS connection. Connection Server Instances should have those intermediate Certificates in its Windows 'Intermediate Certification Authorities' store. See KB 2108294.

Similarly, if a SAML 2.0 authenticator is configured for Connection Server, the Connection Server computer must have installed the root certificate of the signing CA for the SAML 2.0 server certificate.

Overview of Tasks for Setting Up TLS Certificates

To set up TLS server certificates for VMware Horizon 8 servers, you must perform several high-level tasks.

In a pod of replicated Connection Server instances, you must perform these tasks on all instances in the pod.

The procedures for carrying out these tasks are described in the topics that follow this overview.

1 Determine if you need to obtain a new signed TLS certificate from a CA.

   If your organization already has a valid TLS server certificate, you can use that certificate to replace the default TLS server certificate provided with Connection Server. To use an existing certificate, you also need the accompanying private key.

Starting Place	Action
Your organization provided you with a valid TLS server certificate.	Go directly to step 2.
You do not have an TLS server certificate.	Obtain a signed TLS server certificate from a CA.

2 Import the TLS certificate into the Windows local computer certificate store on the VMware Horizon 8 server host.

3 For Connection Server instances modify the certificate Friendly name to **vdm**.

   Assign the Friendly name **vdm** to only one certificate on each VMware Horizon 8 server host.

4 On Connection Server computers, if the root certificate is not trusted by the Windows Server host, import the root certificate into the Windows local computer certificate store.

   In addition, if the Connection Server instances do not trust the root certificates of the TLS server certificates configured for vCenter Server hosts, you also must import those root certificates. Take these steps for Connection Server instances only. You do not have to import the root certificate to vCenter Server hosts.

5 If your server certificate was signed by an intermediate CA, import the intermediate certificates into the Windows local computer certificate store.

   To simplify client configuration, import the entire certificate chain into the Windows local computer certificate store. If intermediate certificates are missing from the VMware Horizon 8 server, they must be configured for clients and computers that launch Horizon Console.

6 If your CA is not well known, configure clients to trust the root and intermediate certificates.

   Also ensure that the computers on which you launch Horizon Console trust the root and intermediate certificates.

7 Determine whether to reconfigure certificate revocation checking.

   Connection Server performs certificate revocation checking on VMware Horizon 8 servers and vCenter Server. Most certificates signed by a CA include certificate revocation information. If your CA does not include this information, you can configure the server not to check certificates for revocation.

If a SAML authenticator is configured for use with a Connection Server instance, Connection Server also performs certificate revocation checking on the SAML server certificate.

Configure Blast Reverse Connection and Message Validation

You can configure Blast to make an outbound TCP connection (referred to as a "reverse connection") from the Agent system to a Blast Secure Gateway running on UAG. By adding a gateway certificate, you can verify that messages are authorized by UAG and have not been tampered with.

Procedure

1 Enable the feature in UAG.

   a In the UAG appliance, go to **General Settings** and select **Edge Service Settings > Horizon Settings**.

   b Click the Settings (gear) icon, then select **Enable Horizon**.

   c In the Horizon Settings pane, turn **Enable XML Signing** to ON and click More to expand the pane.

   d Select the following options: **Enable Blast** and **Blast Reverse Connection Enabled**.

   e Select **Blast Reverse Connection URL Inside** and change the port numbert to 8444.

   f Click Save.

2 Add the certificate.

   a Go to **VMware Horizon > Settings > Servers**.

   b Select the Gateway Certificate tab.

   c Click Add.

   d In the **Add Certificate** dialog, enter a name you want to use to identify the certificate, and copy the certificate details in PEM format into the Certificate field. Click OK.

3 Launch the desktop or application pool from the Client.

4 Check the following:

   - In the registry editor, ReverseConnectionEnabled should be set to 1. This ensures that the reverse connection registry is added to the blast configuration registry.
   - For Reverse Connection Verification, make sure that port 8444 is established from the Agent to UAG, and that the Blast Worker Log shows that the Blast Reverse Connection is enabled and upgraded successfully.

Obtaining a Signed TLS Certificate from a CA

If your organization does not provide you with an TLS server certificate, you must request a new certificate that is signed by a CA.

You can use several methods to obtain a new signed certificate. For example, you can use the Microsoft `certreq` utility to generate a Certificate Signing Request (CSR) and submit a certificate request to a CA.

For an example that shows you how to use `certreq` to accomplish this task, see the *Horizon Integration* document.

For testing purposes, you can obtain a free temporary certificate based on an untrusted root from many CAs.

Important You must follow certain rules and guidelines when you obtain signed TLS certificates from a CA.

- When you generate a certificate request on a computer, make sure that a private key is generated also. When you obtain the TLS server certificate and import it into the Windows local computer certificate store, there must be an accompanying private key that corresponds to the certificate.
- To comply with VMware security recommendations, use the fully qualified domain name (FQDN) that client devices use to connect to the host. Do not use a simple server name or IP address, even for communications within your internal domain.
- Do not generate certificates for servers using a `KeyLength` value under 1024. Client endpoints will not validate a certificate on a server that was generated with a `KeyLength` under 1024, and the clients will fail to connect to the server. Certificate validations that are performed by Connection Server will also fail, resulting in the affected servers showing as red in the Horizon Console dashboard.

For general information about obtaining certificates, consult the Microsoft online help available with the Certificate Snap-in to MMC. If the Certificate Snap-in is not yet installed on your computer, see Add the Certificate Snap-In to MMC.

Obtain a Signed Certificate from a Windows Domain or Enterprise CA

To obtain a signed certificate from a Windows Domain or Enterprise CA, you can use the Windows Certificate Enrollment wizard in the Windows Certificate Store.

This method of requesting a certificate is appropriate if communications between computers remain within your internal domain. For example, obtaining a signed certificate from a Windows Domain CA might be appropriate for server-to-server communications.

If your clients connect to VMware Horizon 8 servers from an external network, request TLS server certificates that are signed by a trusted, third-party CA.

Prerequisites

- Determine the fully qualified domain name (FQDN) that client devices use to connect to the host.

To comply with VMware security recommendations, use the FQDN, not a simple server name or IP address, even for communications within your internal domain.

- Verify that the Certificate snap-in was added to MMC. See Add the Certificate Snap-In to MMC.
- Verify that you have the appropriate credentials to request a certificate that can be issued to a computer or service.

Procedure

1. In the **MMC** window on the Windows Server host, expand the **Certificates (local computer)** node and select the **Personal** folder.
2. From the **Action** menu, go to **All Tasks > Request New Certificate** to display the **Certificate Enrollment** wizard.
3. Select a Certificate Enrollment Policy.
4. Select the types of certificates that you want to request, select the **Make private key exportable** option, and click **Enroll**.
5. Click **Finish**.

Results

The new signed certificate is added to the **Personal > Certificates** folder in the Windows Certificate Store.

What to do next

- Verify that the server certificate and certificate chain were imported into the Windows Certificate Store.
- For a Connection Server instance modify the certificate friendly name to **`vdm`**. See Modify the Certificate Friendly Name.

Configure an Enrollment Service Client Certificate

At installation Horizon Connection Server generates a self-signed enrollment service client certificate. You can replace this self-signed certificate with a CA-signed certificate.

The enrollment service client certificate is used for securing communication between Connection Server and the enrollment server. If you are replacing this certificate with a CA-signed certificate, the new certificate should be imported to the enrollment server and the Root CA certificate should be added to the Trusted Root Certification Authorities store on the enrollment server. For more information see the "Setting Up True SSO" section in the *Horizon Administration* document.

Procedure

1 Generate a CA-signed certificate meeting the requirements below.

Note The root certificate used to generate the client certificate should be added to Trusted Root Certification Authorities store on all Connection Servers in the POD.

- Subject name: Cluster GUID

Note You can find Cluster GUID using the `vdmadmin -C` command or navigating to `Connection Server Cluster GUID` under `HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.\VMware VDM\Node Manager`.

- SAN: Cluster GUID of Horizon pod as DNSName
- EKU: Server authentication, Client authentication
- Set friendly name: `vdm.ec.new`
- Private key must be marked exportable.
- Certificate must be added to **Certificates (Local Computer) > VMware Horizon View Certificates > Certificates**.
- Signature algorithm to use: SHA384/SHA512

2 Import the certificate chain to corresponding folders.

3 Delete the existing cluster certificate with friendly name `vdm.ec`.

4 Restart Connection Server service.

Results

When the Connection Server has accepted the new certificate, the friendly name of the certificate will change from `vdm.ec.new` to `vdm.ec`. If the certificate is not accepted for any reason the old certificate will be moved from LDAP to the Windows certificate store. The other servers in the cluster will fetch this certificate from LDAP.

Configure Horizon Enrollment Server to Use a New TLS Certificate

Configure an Enrollment Server instance to use a CA-signed TLS certificate by importing the server certificate and the entire certificate chain into the Windows local computer certificate store on the Enrollment Server host.

Procedure

1 Generate a CA-signed certificate meeting the requirements below.

- Subject name: FQDN of ES or wildcard
- SAN: FQDN of ES or wildcard

- EKU: Server authentication
- Set friendly name: `vdm.es`
- Private key must be marked exportable.
- Signature algorithm to use: SHA384/SHA512

2 In the MMC window on the Windows Server host, expand the **Certificates (Local Computer)** node and select the **VMware Horizon View Certificates** folder.

3 In the Actions pane, go to **More Actions > All Tasks > Import**.

4 Select the certificate file and click **Open**. To display your certificate file type, you can select its file format from the **File name** drop-down menu.

5 Type the password for the private key that is included in the certificate file.

6 Select **Mark this key as exportable**.

7 Select **Include all extended properties**.

8 Click **Next** and click **Finish**. The new certificate appears in the **Certificates (Local Computer) >Personal >Certificates** folder.

9 Verify that the new certificate contains a private key.

- In the **Certificates (Local Computer) > Personal > Certificates** folder, double-click the new certificate.
- In the General tab of the Certificate Information dialog box, verify that the following statement appears: **You have a private key that corresponds to this certificate.**

10 Modify the certificate Friendly name to `vdm.es`.

11 Restart the VMware Horizon View Enrollment Server Service to make your changes take effect.

Note You must copy the root certificate that was used to generate the Enrollment Server certificate to the Trusted Root Certification Authorities store on the Connection servers.

Configure Horizon Connection Server to Use a New TLS Certificate

To configure a Connection Server instance to use a TLS certificate, you must import the server certificate and the entire certificate chain into the Windows local computer certificate store on the Connection Server host.

In a pod of replicated Connection Server instances, you must import the server certificate and certificate chain on all instances in the pod.

By default, the Blast Secure Gateway (BSG) uses the TLS certificate that is configured for the Connection Server instance on which the BSG is running. If you replace the default, self-signed certificate for a VMware Horizon 8 server with a CA-signed certificate, the BSG also uses the CA-signed certificate.

Important To configure Connection Server to use a certificate, you must change the certificate Friendly name to **vdm**. Also, the certificate must have an accompanying private key.

Procedure

1 Add the Certificate Snap-In to MMC

Before you can add certificates to the Windows Certificate Store, you must add the Certificate snap-in to the Microsoft Management Console (MMC) on the Windows Server host on which the VMware Horizon 8 server is installed.

2 Import a Signed Server Certificate into a Windows Certificate Store

You must import the TLS server certificate into the Windows local computer certificate store on the Windows Server host on which Connection Server is installed.

3 Modify the Certificate Friendly Name

To configure a Connection Server instance to recognize and use an TLS certificate, you must modify the certificate Friendly name to `vdm`.

4 Import a Root Certificate and Intermediate Certificates into a Windows Certificate Store

If the Windows Server host on which Connection Server is installed does not trust the root certificate for the signed TLS server certificate, you must import the root certificate into the Windows local computer certificate store. In addition, if the Connection Server host does not trust the root certificates of the TLS server certificates configured for vCenter Server hosts, you also must import those root certificates.

Add the Certificate Snap-In to MMC

Before you can add certificates to the Windows Certificate Store, you must add the Certificate snap-in to the Microsoft Management Console (MMC) on the Windows Server host on which the VMware Horizon 8 server is installed.

Prerequisites

Verify that the MMC and Certificate snap-in are available on the Windows Server computer on which the VMware Horizon 8 server is installed.

Procedure

1 On the Windows Server computer, click **Start** and type **mmc.exe**.

2 In the **MMC** window, go to **File > Add/Remove Snap-in**.

3 In the **Add or Remove Snap-ins** window, select **Certificates** and click **Add**.

4 In the **Certificates snap-in** window, select **Computer account**, click **Next**, select **Local computer**, and click **Finish**.

5 In the **Add or Remove snap-in** window, click **OK**.

What to do next

Import the TLS server certificate into the Windows Certificate Store.

Import a Signed Server Certificate into a Windows Certificate Store

You must import the TLS server certificate into the Windows local computer certificate store on the Windows Server host on which Connection Server is installed.

Depending on your certificate file format, the entire certificate chain that is contained in the keystore file might be imported into the Windows local computer certificate store. For example, the server certificate, intermediate certificate, and root certificate might be imported.

For other types of certificate files, only the server certificate is imported into the Windows local computer certificate store. In this case, you must take separate steps to import the root certificate and any intermediate certificates in the certificate chain.

For more information about certificates, consult the Microsoft online help available with the Certificate snap-in to MMC.

Note If you off-load TLS connections to an intermediate server, you must import the same TLS server certificate onto both the intermediate server and the off-loaded VMware Horizon server. For details, see "Off-load TLS Connections to Intermediate Servers" in the *Horizon Security* document.

Prerequisites

Verify that the Certificate snap-in was added to MMC. See Add the Certificate Snap-In to MMC.

Procedure

1 In the MMC window on the Windows Server host, expand the **Certificates (Local Computer)** node and select the **Personal** folder.

2 In the Actions pane, go to **More Actions > All Tasks > Import**.

3 In the **Certificate Import** wizard, click **Next** and browse to the location where the certificate is stored.

4 Select the certificate file and click **Open**.

To display your certificate file type, you can select its file format from the **File name** drop-down menu.

5 Type the password for the private key that is included in the certificate file.

6 Select **Mark this key as exportable**.

7 Select **Include all extended properties**.

8 Click **Next** and click **Finish**.

The new certificate appears in the **Certificates (Local Computer) > Personal > Certificates** folder.

9 Verify that the new certificate contains a private key.

a In the **Certificates (Local Computer) > Personal > Certificates** folder, double-click the new certificate.

b In the General tab of the Certificate Information dialog box, verify that the following statement appears: `You have a private key that corresponds to this certificate`.

What to do next

Modify the certificate Friendly name to **vdm**.

Modify the Certificate Friendly Name

To configure a Connection Server instance to recognize and use an TLS certificate, you must modify the certificate Friendly name to `vdm`.

Prerequisites

Verify that the server certificate is imported into the **Certificates (Local Computer) > Personal > Certificates** folder in the Windows Certificate Store. See Import a Signed Server Certificate into a Windows Certificate Store.

Procedure

1 In the MMC window on the Windows Server host, expand the **Certificates (Local Computer)** node and select the **Personal > Certificates** folder.

2 Right-click the certificate that is issued to the VMware Horizon 8 server host and click **Properties**.

3 On the General tab, delete the **Friendly name** text and type **vdm**.

4 Click **Apply** and click **OK**.

5 Verify that no other server certificates in the **Personal > Certificates** folder have a Friendly name of **vdm**.

a Locate any other server certificate, right-click the certificate, and click **Properties**.

b If the certificate has a Friendly name of **vdm**, delete the name, click **Apply**, and click **OK**.

What to do next

Import the root certificate and intermediate certificates into the Windows local computer certificate store.

After all certificates in the chain are imported, you must restart the Connection Server service to make your changes take effect.

Import a Root Certificate and Intermediate Certificates into a Windows Certificate Store

If the Windows Server host on which Connection Server is installed does not trust the root certificate for the signed TLS server certificate, you must import the root certificate into the Windows local computer certificate store. In addition, if the Connection Server host does not trust the root certificates of the TLS server certificates configured for vCenter Server hosts, you also must import those root certificates.

If the Connection Server and vCenter Server certificates are signed by a root CA that is known and trusted by the Connection Server host, and there are no intermediate certificates in your certificate chains, you can skip this task. Commonly used Certificate Authorities are likely to be trusted by the host.

You must import untrusted root certificates on all replicated Connection Server instances in a pod.

Note You do not have to import the root certificate into vCenter Server hosts.

If a server certificate is signed by an intermediate CA, you also must import each intermediate certificate in the certificate chain. To simplify client configuration, import the entire intermediate chain to vCenter Server hosts as well as Connection Server hosts. If intermediate certificates are missing from a Connection Server host, they must be configured for clients and computers that launch Horizon Console. If intermediate certificates are missing from a vCenter Server host, they must be configured for each Connection Server instance.

If you already verified that the entire certificate chain is imported into the Windows local computer certificate store, you can skip this task.

Note If a SAML authenticator is configured for use by a Connection Server instance, the same guidelines apply to the SAML 2.0 authenticator. If the Connection Server host does not trust the root certificate configured for a SAML authenticator, or if the SAML server certificate is signed by an intermediate CA, you must ensure that the certificate chain is imported into the Windows local computer certificate store.

Procedure

1 In the MMC console on the Windows Server host, expand the **Certificates (Local Computer)** node and go to the **Trusted Root Certification Authorities > Certificates** folder.

   - If your root certificate is in this folder, and there are no intermediate certificates in your certificate chain, skip to step 7.
   - If your root certificate is not in this folder, proceed to step 2.

2 Right-click the **Trusted Root Certification Authorities > Certificates** folder and click **All Tasks > Import**.

3 In the **Certificate Import** wizard, click **Next** and browse to the location where the root CA certificate is stored.

4 Select the root CA certificate file and click **Open**.

5 Click **Next**, click **Next**, and click **Finish**.

6 If your server certificate was signed by an intermediate CA, import all intermediate certificates in the certificate chain into the Windows local computer certificate store.

   a Go to the **Certificates (Local Computer) > Intermediate Certification Authorities > Certificates** folder.

   b Repeat steps 3 through 6 for each intermediate certificate that must be imported.

7 Restart the Connection Server service or vCenter Server service to make your changes take effect.

Configure Client Endpoints to Trust Root and Intermediate Certificates

If a VMware Horizon 8 server certificate is signed by a CA that is not trusted by client computers and client computers that access Horizon Console, you can configure all Windows client systems in a domain to trust the root and intermediate certificates. To do so, you must add the public key for the root certificate to the Trusted Root Certification Authorities group policy in Active Directory and add the root certificate to the Enterprise NTAuth store.

For example, you might have to take these steps if your organization uses an internal certificate service.

You do not have to take these steps if the Windows domain controller acts as the root CA, or if your certificates are signed by a well known CA. For well known CAs, the operating system venders preinstall the root certificate on client systems.

If your server certificates are signed by a little-known intermediate CA, you must add the intermediate certificate to the Intermediate Certification Authorities group policy in Active Directory.

For client devices that use other operating systems than Windows, see the following instructions for distributing root and intermediate certificates that users can install:

- For Horizon Client for Mac, see Configure Horizon Client for Mac to Trust Root and Intermediate Certificates.
- For Horizon Client for iOS, see Configure Horizon Client for iOS to Trust Root and Intermediate Certificates.
- For Horizon Client for Android, see documentation on the Google Web site, such as the *Android User's Guide*
- For Horizon Client for Linux, see the Ubuntu documentation

Prerequisites

Verify that the server certificate was generated with a `KeyLength` value of 1024 or larger. Client endpoints will not validate a certificate on a server that was generated with a `KeyLength` under 1024, and the clients will fail to connect to the server.

Procedure

1 On your Active Directory server, use the `certutil` command to publish the certificate to the Enterprise NTAuth store.

For example: **`certutil -dspublish -f path_to_root_CA_cert NTAuthCA`**

2 On the Active Directory server, navigate to the Group Policy Management plug-in and complete the following steps:

a Select **Start > Administrative Tools > Group Policy Management**.

b Expand your domain, right-click **Default Domain Policy**, and click **Edit**.

3 Expand the **Computer Configuration** section and go to **Windows Settings > Security Settings > Public Key Policies**.

4 Import the certificate.

Option	Description
Root certificate	a Right-click **Trusted Root Certification Authorities** and select **Import**. b Follow the prompts in the wizard to import the root certificate (for example, `rootCA.cer`) and click **OK**.
Intermediate certificate	a Right-click **Intermediate Certification Authorities** and select **Import**. b Follow the prompts in the wizard to import the intermediate certificate (for example, `intermediateCA.cer`) and click **OK**.

5 Close the **Group Policy** window.

Results

All systems in the domain now have certificate information in their trusted root certificate stores and intermediate certificate stores that allows them to trust the root and intermediate certificates.

Configure Horizon Client for Mac to Trust Root and Intermediate Certificates

If a server certificate is signed by a CA that is not trusted by computers that run Horizon Client for Mac, you can configure these computers to trust the root and intermediate certificates. You must distribute the root certificate and all intermediate certificates in the trust chain to the client computers.

Procedure

1 Deliver the root certificate and intermediate certificates to the computer that is running Horizon Client for Mac.

2 Open the root certificate on the Mac computer.

  The certificate displays the following message: `Do you want your computer to trust certificates signed by CA name from now on?`

3 Click **Always Trust**

4 Type the user password.

5 Repeat steps 2 through 4 for all intermediate certificates in the trust chain.

Configure Horizon Client for iOS to Trust Root and Intermediate Certificates

If a server certificate is signed by a CA that is not trusted by iPads and iPhones that run Horizon Client for iOS, you can configure the device to trust the root and intermediate certificates. You must distribute the root certificate and all intermediate certificates in the trust chain to the devices.

Procedure

1 Send the root certificate and intermediate certificates as email attachments to the iPad.

2 Open the email attachment for the root certificate and select **Install**.

  The certificate displays the following message:

```
Unverifiable Profile. The authenticity of Certificate name cannot be verified. Installing this profile will change settings on your iPad.

Root Certificate. Installing the certificate Certificate name will add it to the list of trusted certificates on your iPad.
```

3 Select **Install** again.

4 Repeat steps 2 and 3 for all intermediate certificates in the trust chain.

Configuring Certificate Revocation Checking on Server Certificates

Each Connection Server instance performs certificate revocation checking on its own certificate. Each instance also checks the certificates of vCenter Server whenever it establishes a connection to vCenter Server. By default, all certificates in the chain are checked except the root certificate. You can, however, change this default.

If a SAML 2.0 authenticator is configured for use by a Connection Server instance, Connection Server also performs certificate revocation checking on the SAML 2.0 server certificate.

VMware Horizon 8 supports various means of certificate revocation checking, such as certificate revocation lists (CRLs) and the Online Certificate Status Protocol (OCSP). A CRL is a list of revoked certificates published by the CA that issued the certificates. OCSP is a certificate validation protocol that is used to get the revocation status of an X.509 certificate.

With CRLs, the list of revoked certificates is downloaded from a certificate distribution point (DP) that is often specified in the certificate. The server periodically goes to the CRL DP URL specified in the certificate, downloads the list, and checks it to determine whether the server certificate has been revoked. With OCSP, the server sends a request to an OCSP responder to determine the revocation status of the certificate.

When you obtain a server certificate from a third-party certificate authority (CA), the certificate includes one or more means by which its revocation status can be determined, including, for example, a CRL DP URL or the URL for an OCSP responder. If you have your own CA and generate a certificate but do not include revocation information in the certificate, the certificate revocation check fails. An example of revocation information for such a certificate could include, for example, a URL to a Web-based CRL DP on a server where you host a CRL.

If you have your own CA but do not or cannot include certificate revocation information in your certificate, you can choose not to check certificates for revocation or to check only certain certificates in a chain. On the server, with the Windows Registry Editor, you can create the string (REG_SZ) value **CertificateRevocationCheckType**, under `HKLM\Software\VMware, Inc.\VMware VDM\Security`, and set this value to one of the following data values.

Value	Description
1	Do not perform certificate revocation checking.
2	Check only the server certificate. Do not check any other certificates in the chain.
3	Check all certificates in the chain.
4	(Default) Check all certificates except the root certificate.

If this registry value is not set, or if the value set is not valid (that is, if the value is not 1, 2, 3, or 4), all certificates are checked except the root certificate. Set this registry value on each server on which you intend to modify revocation checking. You do not have to restart the system after you set this value.

Note If your organization uses proxy settings for Internet access, you might have to configure your Connection Server computers to use the proxy settings to ensure that certificate revocation checking can be performed for Connection Server instances that are used for secure client connections. If a Connection Server instance cannot access the Internet, certificate revocation checking might fail, and the Connection Server instance might show up as red on the Horizon Console dashboard. For more information, see Troubleshooting Certificate Issues on Horizon Connection Server.

Configure the PCoIP Secure Gateway to Use a New TLS Certificate

To comply with industry or jurisdiction security regulations, you can replace the default TLS certificate that is generated by the PCoIP Secure Gateway (PSG) service with a certificate that is signed by a CA.

In VMware Horizon 8, the PSG service creates a default, self-signed TLS certificate when the service starts up. The PSG service presents the self-signed certificate to clients running Horizon Client 5.2 for Windows or later releases that connect to the PSG.

The PSG also provides a default legacy TLS certificate that is presented to clients running older clients or earlier releases that connect to the PSG.

The default certificates provide secure connections from client endpoints to the PSG and do not require further configuration in Horizon Console. However, configuring the PSG service to use a CA-signed certificate is highly recommended, particularly for deployments that require you to use security scanners to pass compliance testing.

Although it is not required, you are most likely to configure new CA-signed TLS certificates for your servers before you replace the default PSG certificate with a CA-signed certificate. The procedures that follow assume that you already imported a CA-signed certificate into the Windows certificate store for the server on which the PSG is running.

Note If you are using a security scanner for compliance testing, you might want to start by setting the PSG to use the same certificate as the server and scan the VMware Horizon 8 port before the PSG port. You can resolve trust or validation issues that occur during the scan of the View port to ensure that these issues do not invalidate your test of the PSG port and certificate. Next, you can configure a unique certificate for the PSG and do another scan.

Procedure

1 Verify That the Server Name Matches the PSG Certificate Subject Name

When a Connection Server instance is installed, the installer creates a registry setting with a value that contains the FQDN of the computer. You must verify that this value matches the server name part of the URL that security scanners use to reach the PSG port. The server name also must match the subject name or a subject alternate name (SAN) of the TLS certificate that you intend to use for the PSG.

2 Configure a PSG Certificate in the Windows Certificate Store

To replace the default PSG certificate with a CA-signed certificate, you must configure the certificate and its private key in the Windows local computer certificate store on the Connection Server computer on which the PSG is running.

3 Set the PSG Certificate Friendly Name in the Windows Registry

The PSG identifies the TLS certificate to use by means of the server name and certificate Friendly name. You must set the Friendly name value in the Windows registry on the Connection Server computer on which the PSG is running.

4 (Optional) Force a CA-Signed Certificate to Be Used for Connections to the PSG

You can ensure that all client connections to the PSG use the CA-signed certificate for the PSG instead of the default legacy certificate. This procedure is not required to configure a CA-signed certificate for the PSG. Take these steps only if it makes sense to force the use of a CA-signed certificate in your VMware Horizon deployment.

Verify That the Server Name Matches the PSG Certificate Subject Name

When a Connection Server instance is installed, the installer creates a registry setting with a value that contains the FQDN of the computer. You must verify that this value matches the server name part of the URL that security scanners use to reach the PSG port. The server name also must match the subject name or a subject alternate name (SAN) of the TLS certificate that you intend to use for the PSG.

For example, if a scanner connects to the PSG with the URL `https://view.customer.com:4172`, the registry setting must have the value `view.customer.com`. Note that the FQDN of the Connection Server computer that is set during installation might not be the same as this external server name.

Procedure

1. Start the Windows Registry Editor on the Connection Server host where the PCoIP Secure Gateway is running.
2. Navigate to the `HKEY_LOCAL_MACHINE\SOFTWARE\Teradici\SecurityGateway\SSLCertPsgSni` registry setting.
3. Verify that the value of the `SSLCertPsgSni` setting matches the server name in the URL that scanners will use to connect to the PSG and matches the subject name or a subject alternate name of the TLS certificate that you intend to install for the PSG.

   If the value does not match, replace it with the correct value.
4. To make your changes take effect, restart the VMware Horizon PCoIP Secure Gateway service.

What to do next

Import the CA-signed certificate into the Windows local computer certificate store and configure the certificate Friendly name.

Configure a PSG Certificate in the Windows Certificate Store

To replace the default PSG certificate with a CA-signed certificate, you must configure the certificate and its private key in the Windows local computer certificate store on the Connection Server computer on which the PSG is running.

If you intend the PSG to use a unique certificate, you must import the certificate into the Windows local computer certificate store with an exportable private key and set the appropriate Friendly name.

If you intend the PSG to use the same certificate as the server, you do not have to follow this procedure. However, in the Windows registry you must set the server name to match the server certificate subject name and set the Friendly name to **vdm**.

Prerequisites

- Verify that the key length is at least 1024 bits.
- Verify that the TLS certificate is valid. The current time on the server computer must be within the certificate start and end dates.
- Verify that the certificate subject name or a subject alternate name matches the `SSLCertPsgSni` setting in the Windows registry. See Verify That the Server Name Matches the PSG Certificate Subject Name.
- Verify that the Certificate snap-in was added to MMC. See Add the Certificate Snap-In to MMC.
- Familiarize yourself with importing a certificate into the Windows certificate store. See Import a Signed Server Certificate into a Windows Certificate Store.
- Familiarize yourself with modifying the certificate Friendly name. See Modify the Certificate Friendly Name.

Procedure

1. In the MMC window on the Windows Server host, open the **Certificates (Local Computer) > Personal** folder.
2. Import the TLS certificate that is issued to the PSG by selecting **More Actions > All Tasks > Import**.

   Select the following settings in the **Certificate Import** wizard:

   a **Mark this key as exportable**

   b **Include all extendable properties**

   Complete the wizard to finish importing the certificate into the **Personal** folder
3. Verify that the new certificate contains a private key by taking one of these steps:
   - Verify that a yellow key appears on the certificate icon.
   - Double-click the certificate and verify that the following statement appears in the Certificate Information dialog box: `You have a private key that corresponds to this certificate.`.
4. Right-click the new certificate and click **Properties**.
5. On the General tab, delete the **Friendly name** text and type the Friendly name that you have chosen.

   Make sure that you enter exactly the same name in the `SSLCertWinCertFriendlyName` setting in the Windows registry, as described in the next procedure.
6. Click **Apply** and click **OK**.

Results

The PSG presents the CA-signed certificate to client devices that connect to the server over PCoIP.

Note This procedure does not affect legacy client devices. The PSG continues to present the default legacy certificate to legacy client devices that connect the this server over PCoIP.

What to do next

Configure the certificate Friendly name in the Windows registry.

Set the PSG Certificate Friendly Name in the Windows Registry

The PSG identifies the TLS certificate to use by means of the server name and certificate Friendly name. You must set the Friendly name value in the Windows registry on the Connection Server computer on which the PSG is running.

The certificate Friendly name **vdm** is used by all Connection Server instances. By contrast, you can configure your own certificate Friendly name for the PSG certificate. You must configure a Windows registry setting to enable the PSG to match the correct name with the Friendly name that you will set in the Windows certificate store.

The PSG can use the same TLS certificate as the server on which the PSG is running. If you configure the PSG to use the same certificate as the server, the Friendly name must be **vdm**.

The Friendly name value, in both the registry and the Windows certificate store, is case sensitive.

Prerequisites

- Verify that the Window registry contains the correct subject name that is used to reach the PSG port and that matches the PSG certificate subject name or subject alternate name. See Verify That the Server Name Matches the PSG Certificate Subject Name.
- Verify that the certificate Friendly name is configured in the Windows local computer certificate store. See Configure a PSG Certificate in the Windows Certificate Store.

Procedure

1. Start the Windows Registry Editor on the Connection Server computer where the PCoIP Secure Gateway is running.
2. Navigate to the `HKEY_LOCAL_MACHINE\SOFTWARE\Teradici\SecurityGateway` registry key.
3. Add a new String (REG_SZ) value, `SSLCertWinCertFriendlyName`, to this registry key.
4. Modify the `SSLCertWinCertFriendlyName` value and type the certificate Friendly name to be used by the PSG.

   For example: **pcoip**

   If you use the same certificate as the server, the value must be **vdm**.
5. To make your changes take effect, restart the VMware Horizon PCoIP Secure Gateway service.

What to do next

Verify that client devices continue to connect to the PSG.

If you are using a security scanner for compliance testing, scan the PSG port.

Force a CA-Signed Certificate to Be Used for Connections to the PSG

You can ensure that all client connections to the PSG use the CA-signed certificate for the PSG instead of the default legacy certificate. This procedure is not required to configure a CA-signed certificate for the PSG. Take these steps only if it makes sense to force the use of a CA-signed certificate in your VMware Horizon deployment.

In some cases, the PSG might present the default legacy certificate instead of the CA-signed certificate to a security scanner, invalidating the compliance test on the PSG port. To resolve this issue, you can configure the PSG not to present the default legacy certificate to any device that attempts to connect.

Important Performing this procedure prevents all legacy clients from connecting to this server over PCoIP.

Prerequisites

Verify that all client devices that connect to this server, including thin clients, run Horizon Client 5.2 for Windows or Horizon Client or later releases. You must upgrade the legacy clients.

Procedure

1. Start the Windows Registry Editor on the Connection Server computer where the PCoIP Secure Gateway is running.
2. Navigate to the `HKEY_LOCAL_MACHINE\SOFTWARE\Teradici\SecurityGateway` registry key.
3. Add a new String (REG_SZ) value, `SSLCertPresentLegacyCertificate`, to this registry key.
4. Set the `SSLCertPresentLegacyCertificate` value to **0**.
5. To make your changes take effect, restart the VMware Horizon PCoIP Secure Gateway service.

Setting Horizon Console to Trust a vCenter Server Certificate

In the Horizon Console dashboard, you can configure VMware Horizon 8 to trust a vCenter Server certificate that is untrusted.

VMware strongly recommends that you configure vCenter Server to use TLS certificates that are signed by a CA. Alternatively, you can accept the thumbprint of the default certificate for vCenter Server.

Similarly, VMware recommends that you configure SAML 2.0 authenticators to use TLS certificates that are signed by a CA. Alternatively, in the Horizon Console dashboard you can configure VMware Horizon 8 to trust an untrusted SAML 2.0 server certificate by accepting the thumbprint of the default certificate.

Accept the Thumbprint of a Default TLS Certificate

When you add vCenter Server instances to VMware Horizon 8, 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 Chapter 5 Configuring TLS Certificates for VMware Horizon 8 Servers.

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 8. 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.

Benefits of Using TLS Certificates Signed by a CA

A CA is a trusted entity that guarantees the identity of the certificate and its creator. When a certificate is signed by a trusted CA, users no longer receive messages asking them to verify the certificate, and thin client devices can connect without requiring additional configuration.

You can request an TLS server certificate that is specific to a Web domain such as `www.mycorp.com`, or you can request a wildcard TLS server certificate that can be used throughout a domain such as `*.mycorp.com`. To simplify administration, you might choose to request a wildcard certificate if you need to install the certificate on multiple servers or in different subdomains.

Typically, domain-specific certificates are used in secure installations, and CAs usually guarantee more protection against losses for domain-specific certificates than for wildcard certificates. If you use a wildcard certificate that is shared with other services, the security of the VMware Horizon 8 product also depends on the security of those other services. If you use a wildcard certificate, you must ensure that the private key is transferable between servers.

When you replace the default certificate with your own certificate, clients use your certificate to authenticate the server. If your certificate is signed by a CA, the certificate for the CA itself is typically embedded in the browser or is located in a trusted database that the client can access. After a client accepts the certificate, it responds by sending a secret key, which is encrypted with the public key contained in the certificate. The secret key is used to encrypt traffic between the client and the server.

Update the Certificates on a Connection Server Instance

When you receive updated server TLS certificates or intermediate certificates, you import the certificates into the Windows local computer certificate store on each Connection host.

Typically, server certificates expire after 12 months. Root and intermediate certificates expire after 5 or 10 years.

Attention If you are replacing the certificate with a new certificate provider, you must update the trusted root certificates or server thumbprints on the UAG connecting to this server. Failure to do so will result in a total loss of service. For information about updating thumbprints, see "Configure Horizon Settings" in the *Deploying and Configuring VMware Unified Access Gateway* guide.

Prerequisites

- Obtain updated server and intermediate certificates from the CA before the currently valid certificates expire.
- Verify that the Certificate snap-in was added to MMC on the Windows Server on which the Connection Server instance was installed.

Procedure

1. Import the signed TLS server certificate into the Windows local computer certificate store on the Windows Server host.
   a. In the Certificate snap-in, import the server certificate into the **Certificates (Local Computer) > Personal > Certificates** folder.
   b. Select **Mark this key as exportable**.
   c. Click **Next** and click **Finish**.
2. For Connection Server, delete the certificate Friendly name, **vdm**, from the old certificate that was issued to the VMware Horizon 8 server.
   a. Right-click the old certificate and click **Properties**
   b. On the General tab, delete the Friendly name text, **vdm**.
3. For Connection Server, add the certificate Friendly name, **vdm**, to the new certificate that is replacing the previous certificate.
   a. Right-click the new certificate and click **Properties**
   b. On the General tab, in the Friendly name field, type **vdm**.
   c. Click **Apply** and click **OK**.
4. If intermediate certificates are issued to a Connection Server host, import the most recent update to the intermediate certificates into the **Certificates (Local Computer) > Intermediate Certification Authorities > Certificates** folder in the Windows certificate store.
5. Restart the VMware Horizon Connection Server service to make your changes take effect.

Connection Server in FIPS-Compliant Mode Installation Certificate Requirements

A new installation of Connection server in FIPS-compliant mode requires the CA-signed **vdm** certificate to be placed in the Windows certificate store. The installer checks for the presence of this certificate before proceeding with the installation.

The steps to request and install this certificate are the same as described for the current TLS certificate workflow. See Overview of Tasks for Setting Up TLS Certificatesfor details.

The `vdm` certificate requirements are as follows.

- Subject name: FQDN of CS or wildcard matching FQDN
- SAN: FQDN of CS or wildcard matching FQDN
- EKU: Server authentication
- Set friendly name: `vdm`
- Private key must be marked exportable.
- Signature algorithm to use: SHA384/SHA512

Troubleshooting Certificate Issues on Horizon Connection Server

Certificate issues on a Connection Server instance prevent you from connecting to Horizon Console or cause a red health indicator to be displayed for a server.

Problem

You cannot connect to Horizon Console on the Connection Server instance with the problem. When you connect to Horizon Console on another Connection Server instance in the same pod, you see that the dashboard health indicator is red for the problem Connection Server instance.

From the other Connection Server instance, clicking the red health indicator displays `SSL Certificate: Invalid` and `Status:` (blank), indicating that a valid certificate could not be found. The VMware Horizon 8 log file contains a log entry of type ERROR with the following error text: `No qualifying certificates in keystore`.

The VMware Horizon 8 log data is in *<Drive Letter>*`:\ProgramData\VMware\log\ConnectionServer` on the Connection Server instance.

Note This file path is a symbolic link that redirects to the actual location of the log files, which is *<Drive Letter>*`:\ProgramData\VMware\VDM\logs`.

Cause

A certificate might not be installed successfully on a VMware Horizon 8 server for any of the following reasons:

- The certificate is not in the Personal folder in the Windows local computer certificate store.
- The certificate store does not have a private key for the certificate.
- The certificate does not have a friendly name of **vdm**.
- The certificate was generated from a v3 certificate template, for a Windows Server 2008 or later server. VMware Horizon 8 cannot detect a private key, but if you use the Certificate snap-in to examine the Windows certificate store, the store indicates that there is a private key.

Solution

- Verify that the certificate is imported into the Personal folder in the Windows local computer certificate store.

  See Import a Signed Server Certificate into a Windows Certificate Store.
- Verify that the certificate contains a private key.

  See Import a Signed Server Certificate into a Windows Certificate Store.
- Verify that the certificate has a friendly name of **vdm**.

  See Modify the Certificate Friendly Name.
- If the certificate was generated from a v3 certificate template, obtain a valid, signed certificate from a CA that does not use a v3 template.

  See Obtaining a Signed TLS Certificate from a CA.

Configuring VMware Horizon for the First Time

6

After you install the VMware Horizon 8 server software and configure SSL certificates for the servers, you must take a few additional steps to set up a working VMware Horizon 8 environment.

You configure user accounts for vCenter Server, install a VMware Horizon 8 license key or install Horizon Cloud Connector if you have a subscription license, add vCenter Server to your VMware Horizon 8 environment, configure the PCoIP Secure Gateway and secure tunnel, and, optionally, size Windows Server settings to support your VMware Horizon 8 environment.

This chapter includes the following topics:

Configuring an Instant Clone Domain Administrator in Active Directory

When you configure VMware Horizon 8 for the first time and want to use instant clones, you will need to provide an instant-clone user, called the instant-clone domain administrator in Horizon Console.

The instant-clone domain administrator is a user account in Active Directory that allows Connection Server to perform certain operations related to instant clones in Active Directory. Connection Server requires this account to join instant-clone virtual machines to your Active Directory domain. See Create a User Account for Instant-Clone Operations.

After you create and configure this instant-clone domain administrator account, you can specify the user name in Horizon Console.

Configuring User Accounts for vCenter Server

To use vCenter Server with VMware Horizon 8, you must also configure a user account with appropriate vCenter Server privileges. You can create a vCenter Server role with the appropriate privileges and assign that role to the vCenter Server user account.

The list of privileges that you must add to the vCenter Server role varies, depending on whether you use VMware Horizon 8 with or without instant clones. You specify a vCenter Server user when you add vCenter Server to VMware Horizon 8.

Configure a vCenter Server User for VMware Horizon

To configure a user account that allows VMware Horizon 8 to perform operations in vCenter Server, you must assign a vCenter Server role with appropriate privileges to that user.

Prerequisites

- In Active Directory, create a user in the Connection Server domain or a trusted domain. See Creating a User Account for vCenter Server.

Procedure

1. In vCenter Server, prepare a role with the required privileges for the user.
   - You can use the predefined Administrator role in vCenter Server. This role can perform all operations in vCenter Server including instant-clone operations.
   - If you want to use a more limited role than the predefined Administrator role in vCenter Server and you do not plan to use instant clones, you can create a role with the minimum privileges needed by Connection Server to perform vCenter Server operations. In vSphere Client, click **Home > Roles > Add Role**, enter a role name such as **`Horizon Administrator`**, and select privileges for the role.

     See Privileges Required for the vCenter Server User Without Instant Clones.
   - If you want to use a more limited role than the predefined Administrator role in vCenter Server and you plan to use instant clones, you can create a role with the minimum privileges needed by Connection Server to perform vCenter Server operations and instant-clone operations. In vSphere Client, click **Home > Roles > Add Role**, enter a role name such as **`Horizon Instant Clone Administrator`**, and select privileges for the role.

     For vCenter Server privileges that include instant-clone privileges, see Privileges Required for the vCenter Server User With Instant Clones.
2. In vSphere Client, right-click the vCenter Server at the top level of the inventory, click **Add Permission**, and add the vCenter Server user.

   Note You must define the vCenter Server user at the vCenter Server level.
3. From the drop-down menu, select the Administrator role, or the custom Horizon Administrator role that you created, and assign it to the vCenter Server user.

What to do next

In Horizon Console, when you add vCenter Server to VMware Horizon, specify the vCenter Server user. See Add vCenter Server Instances to VMware Horizon 8.

Privileges Required for the vCenter Server User Without Instant Clones

The vCenter Server user must have sufficient vCenter Server privileges to enable Horizon 8 to perform operations in vCenter Server. Create a Horizon Administrator role for the vCenter Server user with the required privileges. These privileges are only applicable if you do not intend to use instant clones.

Table 6-1. Minimum vCenter Server Privileges Required for the Horizon Administrator Role Without Instant Clones

Privilege Group	Privileges to Enable
Folder	Create Folder Delete Folder
Datastore	Allocate space
Virtual Machine	In **Configuration**: ■ **Add or remove device** ■ **Advanced** ■ **Modify device settings** In **Interaction**: ■ **Power Off** ■ **Power On** ■ **Reset** ■ **Suspend** ■ **Perform wipe or shrink operations** In **Inventory**: ■ **Create new** ■ **Create from existing** ■ **Remove** In **Provisioning**: ■ **Customize** ■ **Deploy template** ■ **Read customization specifications** ■ **Clone Template** ■ **Clone Virtual Machine**
Resource	Assign virtual machine to resource pool
Global	Act as vCenter Server
Host	In **Configuration**: ■ **Advanced settings**

Table 6-1. Minimum vCenter Server Privileges Required for the Horizon Administrator Role Without Instant Clones (continued)

Privilege Group	Privileges to Enable
Profile Driven Storage (If you are using vSAN datastores or Virtual Volumes)	(all)
Cryptographic operations	The following privileges are required if you use full clone VMs with a Trusted Platform Module (vTPM) device. ■ **Clone** ■ **Decrypt** ■ **Direct Access** ■ **Encrypt** ■ **Manage KMS** ■ **Migrate** ■ **Register Host**

Privileges Required for the vCenter Server User With Instant Clones

To support instant clones, the vCenter Server user must have privileges in addition to those required to support VMware Horizon 8.

Table 6-2. Minimum vCenter Server Privileges Required for the Horizon Administrator Role with Instant Clones

Privilege Group on vCenter Server	Privileges to Enable
Cryptographic operations	The following privileges are required if you use instant clones VMs with a Trusted Platform Module (vTPM) device. ■ **Clone** ■ **Decrypt** ■ **Direct Access** ■ **Encrypt** ■ **Manage KMS** ■ **Migrate** ■ **Register Host**
Datastore	**Allocate space** **Browse datastore**
Folder	**Create folder** **Delete folder**
Global	**Act as vCenter Server** **Disable methods** **Enable methods** **Manage custom attributes** **Set custom attribute**

Table 6-2. Minimum vCenter Server Privileges Required for the Horizon Administrator Role with Instant Clones (continued)

Privilege Group on vCenter Server	Privileges to Enable
Host	In **Configuration** ■ **Advanced settings** - Required to exchange initial pairing information with agents. In **Inventory** ■ **Modify Cluster** - Required to tie Instant Clone parent VMs to specific hosts.
Network	**Assign network**
Profile Driven Storage	(all--If you are using vSAN datastores or Virtual Volumes)
Resource	**Assign virtual machine to resource pool** **Migrate powered on virtual machine**

Table 6-2. Minimum vCenter Server Privileges Required for the Horizon Administrator Role with Instant Clones (continued)

Privilege Group on vCenter Server	Privileges to Enable
Storage views	Not required
Virtual machine	In **Change Configuration** (all) ■ **Acquire disk lease** ■ **Add existing disk** ■ **Add new disk** ■ **Add or remove device** ■ **Advanced configuration** ■ **Change CPU count** ■ **Change memory** ■ **Change resource** ■ **Change settings** ■ **Change swapfile placement** ■ **Configure Host USB device** ■ **Configure managedBy** ■ **Configure Raw device** ■ **Display connection settings** ■ **Extend virtual disk** ■ **Modify device settings** ■ **Query Fault Tolerance compatibility** ■ **Query unowned files** ■ **Reload from path** ■ **Remove disk** ■ **Rename** ■ **Reset guest information** ■ **Set annotation** ■ **Toggle disk change tracking** ■ **Toggle fork parent** ■ **Upgrade virtual machine compatibility** In **Edit Inventory**: ■ **Create from existing** ■ **Create new** ■ **Move** ■ **Register** ■ **Remove** ■ **Unregister** In **Interaction**: ■ **Connect devices** ■ **Perform wipe or shrink operations** ■ **Power off** ■ **Power on** ■ **Reset** ■ **Suspend**

Table 6-2. Minimum vCenter Server Privileges Required for the Horizon Administrator Role with Instant Clones (continued)

Privilege Group on vCenter Server	Privileges to Enable
	In **Provisioning**: ■ **Allow disk access** ■ **Clone template** ■ **Clone Virtual Machine** ■ **Customize** ■ **Deploy template** ■ **Read customization specifications** In **Snapshot management** ■ **Create snapshot** ■ **Remove snapshot** ■ **Rename snapshot** ■ **Revert snapshot**

Configuring Horizon Connection Server for the First Time

After you install Connection Server, you can configure it based on your requirements.

Horizon Console and Horizon Connection Server

Horizon Console provides a Web-based management interface for VMware Horizon 8.

Horizon Connection Server can have multiple instances that also serve as replica servers. Typically a Connection Server and associated replica servers have a single Horizon Console. Depending on your VMware Horizon 8 deployment, you can get a Horizon Console interface with each instance of a Connection Server. For ease of management, VMware recommends configuring one Horizon Console interface per VMware Horizon 8 pod, which consists of a Connection Server and associated replica servers.

Use the following best practices to use Horizon Console with a Connection Server:

- Use the host name and IP address of the Connection Server to log in to Horizon Console. Use the Horizon Console interface to manage the Connection Server, and any associated replica servers.
- In a pod environment, verify that all administrators use the host name and IP address of the same Connection Server to log in to Horizon Console. Do not use the host name and IP address of the load balancer to access a Horizon Console web page.

- To identify the CPA pod or cluster name of the Connection Server you are working with, you can view the pod or cluster name in the Horizon Console header and in the web browser tab.

Note If you use Unified Access Gateway appliances, you must use the Unified Access Gateway REST API to manage the Unified Access Gateway appliances. For more information, see the *Deploying and Configuring VMware Unified Access Gateway* available at https://docs.vmware.com/en/Unified-Access-Gateway/index.html.

Log In to Horizon Console

To perform desktop or application pool deployment tasks, or monitoring and troubleshooting tasks, you must log in to Horizon Console. You access Horizon Console by using a secure (TLS) connection.

Prerequisites

- Verify that Horizon Connection Server is installed on a dedicated computer.
- Verify that you are using a Web browser supported by Horizon Console. For more information about supported Web browsers, see Horizon Console Requirements - Install Only.

Procedure

1. Open your Web browser and enter the following URL, where *server* is the host name of the Connection Server instance.

   `https://server/admin`

   Note You can use the IP address if you have to access a Connection Server instance when the host name is not resolvable. However, the contacted host will not match the TLS certificate that is configured for the Connection Server instance, resulting in blocked access or access with reduced security. VMware recommends using the FQDN instead of the IP address.

   Your access to Horizon Console depends on the type of certificate that is configured on the Connection Server computer.

If you open your Web browser on the Connection Server host, use **`https://127.0.0.1`** to connect, not **`https://localhost`**. This method improves security by avoiding potential DNS attacks on the `localhost` resolution.

Note If using an older Web browser to launch Horizon Console, a message appears indicating that using a modern browser will provide a better user experience. You can click on your preferred Web browser from the options displayed to download it.

Option	Description
You configured a certificate signed by a CA for Connection Server.	When you first connect, your Web browser displays the VMware Horizon 8 page.
The default, self-signed certificate supplied with Connection Server is configured.	When you first connect, your Web browser might display a page warning that the security certificate associated with the address is not issued by a trusted certificate authority. Click **Ignore** to continue using the current TLS certificate.

2 Log in as a user with credentials to access the Administrators account.

You make an initial assignment to the Administrators role when you install a standalone Connection Server instance or the first Connection Server instance in a replicated group. By default, the account that you use to install Connection Server is selected, but you can change this account to the Administrators local group or to a domain global group.

If you chose the Administrators local group, then you can use any domain user added to this group directly or through global group membership. You cannot use local users added to this group.

3 Optionally, to remember the user name for every login, select **Remember user name**.

4 Click **Sign In**.

What to do next

You can also right-click any link in Horizon Console to open in another web browser tab.

Install the Term Product License Key in Horizon Console

If you use a term license, you must enter a product license key.

Note The product license key is not required if you have a VMware Horizon 8 subscription license. For more information about subscription licenses, see Enabling VMware Horizon 8 for Subscription Licenses and Horizon Control Plane Services.

You do not have to configure a license key when you install a replicated Connection Server instance. Replicated instances use the common license key stored in the Horizon LDAP configuration.

Note Connection Server requires a valid license key. The product license key is a 25-character key.

Horizon term licenses include an additional 30 days beyond the written expiration date for continued access. You can use these 30 days to repurchase a Horizon license and install before the original term license expires.

Example: If you purchased a one year Horizon term license on 10 Oct 2021, the 30-day grace period means your license expires at 12:00 on 11 Nov 2022.

Procedure

1 In Horizon Console, select **Settings > Product Licensing and Usage**.

2 In the **Licensing Settings** panel, click **Edit License**.

3 Enter the license serial number and click **OK**.

4 Verify the license expiration date.

5 Verify that the component licenses are enabled or disabled, based on the edition of VMware Horizon 8 that your product license entitles you to use.

Enabling VMware Horizon 8 for Subscription Licenses and Horizon Control Plane Services

If you are using a subscription license, you can enable your VMware Horizon 8 deployment to connect to the Horizon Control Plane. You can optionally use the SaaS services provided by the Horizon Control Plane. You must first use the Horizon Cloud Connector virtual appliance to connect your VMware Horizon 8 deployment with the Horizon Control Plane.

Subscription Licenses for VMware Horizon

VMware Horizon 8 subscription licenses are available through the Horizon universal license, which is available standalone and as part of the Workspace ONE Enterprise bundle.

The VMware Horizon 8 subscription license provides the same VMware Horizon 8 product components with more flexible deployment options. While the perpetual license only allows you to deploy VMware Horizon 8 on-premises or in private datacenters, the VMware Horizon 8 subscription license gives the following additional benefits:

- Ability to deploy into public clouds with VMware SDDC service such as VMware Cloud on AWS, Azure VMware Solution, Google VMware Cloud Engine, and Oracle VMware Cloud Solution.
- Services available through the Horizon Control Plane.

Note The subscription license for VMware Horizon 8 is managed by VMware only after you deploy the Horizon Cloud Connector virtual appliance. You will not receive the license key for VMware Horizon 8 with this subscription license. However, you will receive license keys for vSphere, vCenter Server, vSAN, App Volumes, and Dynamic Environment Manager with this subscription license. You will receive these keys in an email with the following subject: Welcome to VMware Horizon On-Premises Subscription.

Horizon Control Plane for Horizon Pods

After you configure the Horizon Cloud Connector virtual appliance to connect your pod to the Horizon Control Plane, you have the option to leverage the management, features, and workflows that are provided by Horizon Control Plane and which are available to you according to that subscription license. For information about those services, see Introduction to Horizon Cloud in the VMware Control Plane documentation.

Horizon Cloud Connector and Horizon Control Plane can be used for any Horizon pods, whether they are deployed on-premises or in public clouds.

Note For multi-location pods, Horizon assigns the deployment type of the connection server as the pod type and the location of the connection server as the pod location.

Horizon Cloud Connector

The Horizon Cloud Connector is a virtual appliance that is deployed alongside the VMware Horizon 8 pod and pairs the pod with the Horizon Control Plane. Horizon Cloud Connector is a required component that bridges your VMware Horizon 8 pods with Horizon Cloud Service.

You must have an active My VMware account to purchase a VMware Horizon 8 license from https://my.vmware.com. You then receive an email with the link to download the Horizon Cloud Connector as an OVA file.

When you deploy the Horizon Cloud Connector virtual appliance from vSphere Client, the Horizon Cloud Connector virtual appliance connects the Connection Server to Horizon Control Plane to manage the VMware Horizon 8 subscription license and other services. With a subscription license, you do not need to manually enter a license key for the VMware Horizon 8 product activation. However, you do need to use the license keys to activate supporting components such as vSphere, vCenter Server, App Volumes, and others.

Note The Horizon Cloud Connector virtual appliance does not support an IPv6 environment.

For more information about deploying the Horizon Cloud Connector virtual appliance and completing that connection between a Horizon pod with Horizon Control Plane, see the following topics in the Horizon Control Plane documentation:

- End-to-End Workflow When Your Very First Cloud-Connected Pod is from Connecting Horizon Cloud with an Existing Manually Deployed Horizon Pod
- Connect Horizon Cloud with an Existing Manually Deployed Horizon Pod

Add vCenter Server Instances to VMware Horizon 8

If you plan to deploy VMware Horizon 8 on a VMware virtualization platform, you must configure VMware Horizon 8 to connect to the vCenter Server instances in your deployment. vCenter Server creates and manages the virtual machines that VMware Horizon 8 uses in desktop pools.

If you run vCenter Server instances in a Linked Mode group, you must add each vCenter Server instance to VMware Horizon 8 separately. Horizon 8 supports one or multiple vCenter Servers added to the same Horizon pod, as well as a single vCenter Server across multiple Horizon pods in a Cloud Pod Architecture environment.

VMware Horizon 8 connects to the vCenter Server instance using a secure channel (TLS).

Warning After adding a vCenter Server to Horizon and creating managed desktop pools or farms, do not rename any vSphere objects in use by those pools or farms, such as Data Centers, Clusters, Datastores, or Resource Pools. Renaming these objects can cause Horizon to lose its reference to those objects, causing future provisioning and power operations to fail. Rename vSphere objects before creating pools or farms, or when those objects are not referenced by existing Horizon pools or farms. For more information, see VMware Knowledge Base article 1015100.

Prerequisites

- Install the Horizon perpetual license key. Or if you are using a subscription license, deploy the Horizon Cloud Connector to enable your subscription license.
- Prepare a vCenter Server user with permission to perform the operations in vCenter Server that are necessary to support VMware Horizon 8.
- Verify that there is a TLS server certificate installed on the vCenter Server host. In a production environment, install a valid certificate that is signed by a trusted Certificate Authority (CA).

  In a testing environment, you can use the default certificate that is installed with vCenter Server, but you must accept the certificate thumbprint when you add vCenter Server to VMware Horizon 8.
- Verify that all Connection Server instances in the replicated group trust the root CA certificate for the server certificate that is installed on the vCenter Server host. Check if the root CA certificate is in the **Trusted Root Certification Authorities > Certificates** folder in the Windows local computer certificate stores on the Connection Server hosts. If it is not, import the root CA certificate into the Windows local computer certificate stores.

  See Import a Root Certificate and Intermediate Certificates into a Windows Certificate Store.
- Verify that the vCenter Server instance contains ESXi hosts. If no hosts are configured in the vCenter Server instance, you cannot add the instance to VMware Horizon 8.
- Verify that the domain administrator account that you use as the vCenter Server user was explicitly assigned permissions to log in to vCenter Server by a vCenter Server local user.
- Familiarize yourself with the settings that determine the maximum operations limits for vCenter Server.

Procedure

1 In Horizon Console, navigate to **Settings > Servers**.

2 On the **vCenter Server** tab, click **Add**.

3 In the vCenter Server Settings **Server address** text box, enter the fully qualified domain name (FQDN) of the vCenter Server instance.

   The FQDN includes the host name and the domain name. For example, in the FQDN ***myserverhost.companydomain.com***, ***myserverhost*** is the host name and ***companydomain.com*** is the domain.

   Note If you enter a server by using a DNS name or URL, VMware Horizon 8 does not perform a DNS lookup to verify whether an administrator previously added this server to VMware Horizon 8 by using its IP address. A conflict arises if you add a vCenter Server with both its DNS name and its IP address.

4 Enter the name of the vCenter Server user.

   For example: **domain\user** or **user@domain.com**

5 Enter the vCenter Server user password.

6 (Optional) Enter a description for this vCenter Server instance.

7 Enter the TCP port number.

   The default port is 443.

8 Select the deployment type for your vCenter from the drop-down menu.

Deployment Type	Description
AWS	vCenter is deployed on VMware Cloud on AWS
Azure	vCenter is deployed on Azure VMware Solution
DELLEMC	vCenter is deployed on VMware Cloud on Dell EMC
Google	vCenter is deployed on Google Cloud VMware Engine
Oracle	vCenter is deployed on Oracle Cloud VMware Solution
General	vCenter is deployed on-premises or in an environment not listed above

9 Under Advanced Settings, set the concurrent operations limits for vCenter Server operations.

10 Click **Next** and follow the prompts to complete the wizard.

What to do next

If VMware Horizon 8 uses multiple vCenter Server instances, repeat this procedure to add the other vCenter Server instances.

Register Gateways in Horizon Console

Horizon Clients connect through a gateway or Unified Access Gateway appliance that you register in Horizon Console.

You can register or unregister gateways in Horizon Console. To unregister the gateway, select the gateway or Unified Access Gateway appliance and click **Unregister**.

Procedure

1 In Horizon Console, select **Settings > Servers**.

2 On the **Gateways** tab, click **Register**.

3 Enter the Unified Access Gateway appliance ID provided during the gateway configuration.

4 Click **OK**.

Add an Instant-Clone Domain Administrator

Before you create an instant-clone desktop pool, you must add an instant-clone domain administrator to VMware Horizon 8.

For more information about configuring an instant-clone domain administrator in Active Directory, see Configuring an Instant Clone Domain Administrator in Active Directory.

Procedure

1 In the Horizon console, select **Settings > Domains > Instant Clone Engine Domain Accounts**.

2 Click **Add**.

3 Enter the domain, user name, and password for the instant-clone domain administrator.

Configuring View Storage Accelerator for vCenter Server

You can enable View Storage Accelerator on desktop pools that contain instant clones and desktop pools that contain full virtual machines. This feature uses the Content Based Read Cache (CBRC) feature in ESXi hosts. Instead of reading the entire OS or application from the storage system over and over, a host can read common data blocks from cache.

CBRC uses ESXi host memory to cache virtual machine disk data, thus reducing IOPS required and improve performance during boot storms, when many machines start up or run anti-virus scans at once. By reducing the number of IOPS during boot storms, View Storage Accelerator lowers the demand on the storage array, which lets you use less storage I/O bandwidth to support your Horizon deployment. The feature is also beneficial when administrators or users load applications or data frequently.

You can enable or disable View Storage Accelerator globally and then enable or disable it for individual desktop pools. The steps to enable or disable View Storage Accelerator are different for instant-clone desktop pools and desktop pools that contain full virtual machines.

Important If you plan to use this feature and you are using multiple Horizon pods that share some ESXi hosts, you must enable the View Storage Accelerator feature for all pools that are on the shared ESXi hosts. Having inconsistent settings in multiple pods can cause instability of the virtual machines on the shared ESXi hosts.

Note Native NFS snapshot technology (VAAI) and VVOL are not supported in pools that are enabled for View Storage Accelerator.

Enable View Storage Accelerator Globally in Horizon Console

You can enable View Storage Accelerator globally for all desktop pools.

Prerequisites

- Verify that the vCenter Server user was assigned the **Host > Configuration > Advanced settings** privilege in vCenter Server.

  See Configuring User Accounts for vCenter Server.

Procedure

1. In Horizon Console, navigate to **Settings > Servers**.
2. On the **vCenter Server** tab, click **Add** and complete the **Add vCenter Server** wizard pages that precede the **Storage Settings** page.
3. On the **Storage Settings** page, select **Enable View Storage Accelerator**.

   This option is selected by default.
4. Specify a default host cache size.

   The default cache size applies to all ESXi hosts that are managed by this vCenter Server instance.

   The default value is 1,024MB. The cache size must be between 100MB and 32,768MB.
5. To specify a different cache size for an individual ESXi host, select an ESXi host and click **Edit cache size**.
   a. In the Host cache dialog box, check **Override default host cache size**.
   b. Type a **Host cache size** value between 100MB and 32,768MB and click **OK**.
6. On the Storage Settings page, click **Next**.
7. After reviewing the settings on the **Ready to Complete** page, click **Submit**.

Enabling View Storage Accelerator for Individual Desktop Pools

For instant clone pools, View Storage Accelerator is only needed for replica virtual machines. This is enabled automatically for individual pools and cannot be turned off on a pool level.

To complete View Storage Accelerator settings in VMware Horizon 8, configure View Storage Accelerator for desktop pools. See "Configure View Storage Accelerator for Desktop Pools" in the *Windows Desktops and Applications in Horizon* document.

To disable, you must disable View Storage Accelerator globally. See Enable View Storage Accelerator Globally in Horizon Console. However, this would also disable the feature for desktop pools that contain full virtual machines as well.

For desktop pools that contain full virtual machines, View Storage Accelerator is enabled for desktop pools by default. The feature can be disabled or enabled when you create or edit a pool. The best approach is to enable this feature when you first create a desktop pool.

Concurrent Operations Limits for vCenter Server

When you add vCenter Server to VMware Horizon 8 or edit the vCenter Server settings, you can configure several options that set the maximum number of concurrent operations that are performed by vCenter Server.

You configure these options in the Advanced Settings panel on the **vCenter Server Settings** page in the **Add vCenter Server** wizard.

Table 6-3. Concurrent Operations Limits for vCenter Server

Setting	Description
Max concurrent vCenter provisioning operations	Determines the maximum number of concurrent requests that Connection Server can make to provision and delete full virtual machines in this vCenter Server instance. The default value is 20. This setting applies to automated pools of full virtual machines only.
Max concurrent power operations	Determines the maximum number of concurrent power operations (startup, shutdown, suspend, and so on) that can take place on virtual machines managed by Connection Server in this vCenter Server instance. The default value is 50. For guidelines for calculating a value for this setting, see Setting a Concurrent Power Operations Rate to Support Remote Desktop Logon Storms This setting applies to automated pools of full virtual machines.
Max concurrent maintenance operations	Determines the maximum number of concurrent maintenance operations that can take place. The default value is 12. Remote desktops that have active sessions must be logged off before a maintenance operation can begin. If you force users to log off as soon as a maintenance operation begins, the maximum number of concurrent operations on remote desktops that require logoffs is half the configured value. For example, if you configure this setting as 24 and force users to log off, the maximum number of concurrent operations on remote desktops that require logoffs is 12. This setting applies to instant clones.
Max concurrent Instant Clone Engine operations	Determines the maximum number of concurrent creation and deletion operations that can take place on instant clones managed by this vCenter Server instance. This setting applies to instant clones only.

Setting a Concurrent Power Operations Rate to Support Remote Desktop Logon Storms

The **Max concurrent power operations** setting governs the maximum number of concurrent power operations that can occur on remote desktop virtual machines in a vCenter Server instance. This limit is set to 50 by default. You can change this value to support peak power-on rates when many users log on to their desktops at the same time.

As a best practice, you can conduct a pilot phase to determine the correct value for this setting. For planning guidelines, see "Architecture Design Elements and Planning Guidelines" in the *Horizon Overview and Deployment Planning* document.

The required number of concurrent power operations is based on the peak rate at which desktops are powered on and the amount of time it takes for the desktop to power on, boot, and become available for connection. In general, the recommended power operations limit is the total time it takes for the desktop to start multiplied by the peak power-on rate.

For example, the average desktop takes two to three minutes to start. Therefore, the concurrent power operations limit should be 3 times the peak power-on rate. The default setting of 50 is expected to support a peak power-on rate of 16 desktops per minute.

The system waits a maximum of five minutes for a desktop to start. If the start time takes longer, other errors are likely to occur. To be conservative, you can set a concurrent power operations limit of 5 times the peak power-on rate. With a conservative approach, the default setting of 50 supports a peak power-on rate of 10 desktops per minute.

Logons, and therefore desktop power on operations, typically occur in a normally distributed manner over a certain time window. You can approximate the peak power-on rate by assuming that it occurs in the middle of the time window, during which about 40% of the power-on operations occur in 1/6th of the time window. For example, if users log on between 8:00 AM and 9:00 AM, the time window is one hour, and 40% of the logons occur in the 10 minutes between 8:25 AM and 8:35 AM. If there are 2,000 users, 20% of whom have their desktops powered off, then 40% of the 400 desktop power-on operations occur in those 10 minutes. The peak power-on rate is 16 desktops per minute.

Accept the Thumbprint of a Default TLS Certificate

When you add vCenter Server instances to VMware Horizon 8, you must ensure that the TLS certificates that are used for the 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 instance 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.

Note If you install vCenter Server on the same Windows Server host, they can use the same TLS certificate, but you must configure the certificate separately for each component.

For details about configuring TLS certificates, see Chapter 5 Configuring TLS Certificates for VMware Horizon 8 Servers.

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 and 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.

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 instance.
   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 instance.

   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.

Configuring Horizon Client Connections

Client endpoints communicate with a Connection Server host over secure connections.

The initial client connection, which is used for user authentication and remote desktop and application selection, is created over HTTPS when a user provides a domain name to Horizon Client. If firewall and load balancing software are configured correctly in your network environment, this request reaches the Connection Server host. With this connection, users are authenticated and a desktop or application is selected, but users have not yet connected to the remote desktop or application.

When users connect to remote desktops and applications, by default the client makes a second connection to the Connection Server host. This connection is called the tunnel connection because it provides a secure tunnel for carrying RDP and other data over HTTPS.

When users connect to remote desktops and applications with the PCoIP display protocol, the client can make a further connection to the PCoIP Secure Gateway on the Connection Server host. The PCoIP Secure Gateway ensures that only authenticated users can communicate with remote desktops and applications over PCoIP.

You can also provide secure connections to users connect to remote desktops and applications with the VMware Blast display protocol and to external users who use HTML Access to connect to remote desktops. The Blast Secure Gateway ensures that only authenticated users can communicate with remote desktops.

Depending on the type of client device being used, additional channels are established to carry other traffic such as USB redirection data to the client device. These data channels route traffic through the secure tunnel if it is enabled.

When the secure tunnel and secure gateways are disabled, desktop and application sessions are established directly between the client device and the remote machine, bypassing the Connection Server host. This type of connection is called a direct connection.

Desktop and application sessions that use direct connections remain connected even if Connection Server is no longer running.

Typically, to provide secure connections for external clients that connect to a Connection Server host over a WAN, you enable the secure tunnel, the PCoIP Secure Gateway, and the Blast Secure Gateway. You can disable the secure tunnel and the secure gateways to allow internal, LAN-connected clients to establish direct connections to remote desktops and applications.

If you enable only the secure tunnel or only one secure gateway, a session might use a direct connection for some traffic but send other traffic through the Connection Server host, depending on the type of client being used.

TLS is required for all client connections to Connection Server hosts.

Enable Host Redirection

Use the **Enable Host Redirection** setting to set the load balancer name and enable HTTP host redirection capability.

When an HTTP request from a load balancer host reaches the Connection Server, the Connection Server responds with an external HTTP redirection URL. For subsequent requests, the Horizon Client directly connects to the Connection Server using the external URL, thereby minimizing misroutes that might occur at the load balancer.

Note the following:

- You can enter multiple load balancer host names.
- Load balancer host names are also used in Origin Checking. For more information, see https://kb.vmware.com/s/article/85801.

- Unified Access Gateway (UAG) has a feature that rewrites the origin header coming from the client to match the URL it is using to forward requests to the connection server. For more information, see "Configure Horizon Settings" in the *Deploying and Configuring VMware Unified Access Gateway* document on the Unified Access Gateway Documentation site.

Important You must restart the server is to ensure that the load balancer hostname values take effect. If an existing connection server already has `balancedHost` set in `locked.properties`, that setting takes precedence when you are on the new version of Horizon 8.

Procedure

1. In Horizon Console, select **Settings > Servers**.
2. On the **Connection Servers** tab, select a Connection Server instance and click **Edit**.
3. On the **General** tab, select the **Enable Host Redirection** check box.
4. Enter the load balancer name in the text box and click the plus sign ("+") to the right of the text box to add the host.

Results

The host name you entered appears below the text box. You can remove it by clicking the "x" next to the name.

Configure the Secure Tunnel and PCoIP Secure Gateway

When the secure tunnel is enabled, Horizon Client makes a second HTTPS connection to the Connection Server when users connect to a remote desktop.

When the PCoIP Secure Gateway is enabled, Horizon Client makes a further secure connection to the Connection Server host when users connect to a remote desktop with the PCoIP display protocol.

Note If you use Unified Access Gateway appliances, you must disable the secure gateways on Connection Server instances and enable these gateways on the Unified Access Gateway appliances. For more information, see the *Deploying and Configuring VMware Unified Access Gateway* document available at https://docs.vmware.com/en/Unified-Access-Gateway/index.html.

When the secure tunnel or PCoIP Secure Gateway is not enabled, a session is established directly between the client system and the remote desktop virtual machine, bypassing the Connection Server. This type of connection is called a direct connection.

Important In a network configuration in which external clients connect directly to a Connection Server host, you enable or disable the secure tunnel and PCoIP Secure Gateway by editing that Connection Server instance in Horizon Console.

Procedure

1 In Horizon Console, select **Settings > Servers**.

2 On the **Connection Servers** tab, select a Connection Server instance and click **Edit**.

3 On the **General** tab, configure use of the secure tunnel.

Option	Description
Enable the secure tunnel	Select **Use Secure Tunnel connection to machine**.
Disable the secure tunnel	Deselect **Use Secure Tunnel connection to machine**.

The secure tunnel is enabled by default.

4 Configure use of the PCoIP Secure Gateway.

Option	Description
Enable the PCoIP Secure Gateway	Select **Use PCoIP Secure Gateway for PCoIP connections to machine**
Disable the PCoIP secure Gateway	Deselect **Use PCoIP Secure Gateway for PCoIP connections to machine**

The PCoIP Secure Gateway is disabled by default.

5 Click **OK** to save your changes.

Configure the Blast Secure Gateway

In Horizon Console, you can configure the use of the Blast Secure Gateway to provide secure access to remote desktops and applications, either through HTML Access or through client connections that use the VMware Blast display protocol.

The Blast Secure Gateway includes Blast Extreme Adaptive Transport (BEAT) networking, which dynamically adjusts to network conditions such as varying speeds and packet loss.

- Blast Secure Gateway supports BEAT networking only when running on a Unified Access Gateway appliance.
- Horizon Clients using IPv4 and Horizon Clients using IPv6 can be handled concurrently on TCP port 8443 and on UDP port 8443 (for BEAT) when connecting to a Unified Access Gateway appliance version 3.3 or later.
- Horizon Clients that use a typical network condition must connect to a Connection Server (BSG disabled) or versions later than 2.8 of an Unified Access Gateway appliance. If Horizon Client uses a typical network condition to connect to a Connection Server (BSG enabled) or versions earlier than 2.8 of an Unified Access Gateway appliance, the client automatically senses the network condition and falls back to TCP networking.
- Horizon Clients that use a poor network condition must connect to version 2.9 or later of an Unified Access Gateway appliance (with UDP Tunnel Server Enabled). If Horizon Client uses a poor network condition to connect to the Connection Server (BSG enabled) or versions earlier than 2.8 of an Unified Access Gateway appliance, the client automatically senses the network condition and falls back to TCP networking.

- Horizon Clients that use a poor network condition to connect to Connection Server (BSG disabled) or version 2.9 or later of Unified Access Gateway appliance (without UDP Tunnel Server Enabled), or version 2.8 of Unified Access Gateway appliance, the client automatically senses the network condition and falls back to the typical network condition.

For more information, see the Horizon Client documentation at https://docs.vmware.com/en/VMware-Horizon-Client/index.html.

Note If you use Unified Access Gateway appliances, you must disable the secure gateways on Connection Server instances and enable these gateways on the Unified Access Gateway appliances. For more information, see the *Deploying and Configuring VMware Unified Access Gateway* document available at https://docs.vmware.com/en/Unified-Access-Gateway/index.html.

When the Blast Secure Gateway is not enabled, client devices and client Web browsers use the VMware Blast Extreme protocol to establish direct connections to remote desktop virtual machines and applications, bypassing the Blast Secure Gateway.

Prerequisites

If users select remote desktops by using VMware Workspace ONE Access, verify that VMware Workspace ONE Access is installed and configured for use with Connection Server and that Connection Server is paired with a SAML 2.0 Authentication server.

Procedure

1. In Horizon Console, select **Settings > Servers**.
2. On the **Connection Servers** tab, select a Connection Server instance and click **Edit**.
3. Configure use of the Blast Secure Gateway.

Option	Description
Enable the Blast Secure Gateway	Select **Use Blast Secure Gateway for Blast connections to machine**
Enable the Blast Secure Gateway for HTML Access	Select **Use Blast Secure Gateway for only HTML Access Blast connections to machine**
Disable the Blast Secure Gateway	Select **Do not use Blast Secure Gateway**

   The Blast Secure Gateway is enabled by default.

4. Click **OK** to save your changes.

Set the External URLs for Horizon Connection Server Instances

You can use Horizon Console to configure the external URLs for Connection Server instances.

By default, a Connection Server host can be contacted only by tunnel clients that reside within the same network. Tunnel clients that run outside of your network must use a client-resolvable URL to connect to a Connection Server host.

When users connect to remote desktops with the PCoIP display protocol, Horizon Client can make a further connection to the PCoIP Secure Gateway on the Connection Server host. To use the PCoIP Secure Gateway, a client system must have access to an IP address that allows the client to reach the Connection Server host. You specify this IP address in the PCoIP external URL.

A third URL allows users to make secure connections through the Blast Secure Gateway.

The secure tunnel external URL, PCoIP external URL, and Blast external URL must be the addresses that client systems use to reach this host.

Prerequisites

- Verify that the secure tunnel connections and the PCoIP Secure Gateway are enabled on the Connection Server instance. See Configure the Secure Tunnel and PCoIP Secure Gateway.
- To set the Blast external URL, verify that the Blast Secure Gateway is enabled on the Connection Server instance. See Configure the Blast Secure Gateway.

Procedure

1. In Horizon Console, select **Settings > Servers**.
2. On the **Connection Servers** tab, select the Connection Server instance and click **Edit**.
3. Type the secure tunnel external URL in the **External URL** text box.

   The URL must contain the protocol, client-resolvable host name and port number.

   For example: https://horizon.example.com:443

   Note You can use the IP address if you have to access a Connection Server instance when the host name is not resolvable. However, the host that you contact will not match the TLS certificate that is configured for the Connection Server instance, resulting in blocked access or access with reduced security.
4. Type the PCoIP Secure Gateway external URL in the **PCoIP External URL** text box.

   Specify the PCoIP external URL as an IP address with the port number 4172. Do not include a protocol name.

   For example: `10.20.30.40:4172`

   The URL must contain the IP address and port number that a client system can use to reach this Connection Server instance.
5. Type the Blast Secure Gateway external URL in the **Blast External URL** text box.

   The URL must contain the HTTPS protocol, client-resolvable host name, and port number.

   For example: `https://myserver.example.com:8443`

   By default, the URL includes the FQDN of the secure tunnel external URL and the default port number, 8443. The URL must contain the FQDN and port number that a client system can use to reach this host.
6. Verify that all addresses in this dialog allow client systems to reach this host.

7 Click **OK** to save your changes.

Results

The external URLs are updated immediately. You do not need to restart the Connection Server for the changes to take effect.

Give Preference to DNS Names When Horizon Connection Server Returns Address Information

By default, when sending the addresses of desktop machines and RDS hosts to clients and gateways, Horizon Connection Server gives preference to IP addresses. You can change this default behavior with an LDAP attribute that tells Horizon Connection Server to give preference to DNS names. In certain environments, having Connection Server return DNS names to clients and gateways can provide additional flexibility in designing a network infrastructure.

The LDAP attribute affects clients that run Horizon Client for Windows, HTML Access, and secure gateways on Connection Server instances.

Prerequisites

See the Microsoft TechNet Web site for information on how to use the ADSI Edit utility on your Windows Server operating system version.

Procedure

1 Start the ADSI Edit utility on your Connection Server computer.

2 In the console tree, select **Connect to**.

3 In the **Select or type a Distinguished Name or Naming Context** text box, type the distinguished name **DC=vdi, DC=vmware, DC=int**.

4 In the **Select or type a domain or server** text box, select or type **`localhost:389`** or the fully qualified domain name (FQDN) of the Connection Server computer followed by port 389.

   For example: `localhost:389 or mycomputer.mydomain.com:389`

5 On the object **OU=Properties > OU=Global > CN=Common**, set the **pae-PreferDNS** attribute value to 1.

   When this attribute is set to 1, Connection Server returns a DNS name, if a DNS name is available and the recipient supports name resolution. Otherwise, Connection Server returns an IP address, if an IP address of the correct type for your environment (IPv4 or IPv6) is available.

   When this attribute is not set or is set to 0, Connection Server returns an IP address, if an IP address of the correct type is available. Otherwise, an IP address compatibility error is returned.

Allow HTML Access Through a Load Balancer

Connection Server instances that are directly behind a load balancer or load-balanced gateway must know the address by which browsers will connect to the load balancer when users use HTML Access.

For Connection Server instances that are directly behind a gateway, perform the procedure described in Allow HTML Access Through a Gateway.

You must perform this procedure for each Connection Server that is behind the load balancer or load-balanced gateway.

Procedure

1. Create or edit the `locked.properties` file in the gateway configuration folder on the Connection Server host.

   For example: *`install_directory`*`\VMware\VMware View\Server\sslgateway\conf\locked.properties`

2. Add the `balancedHost` property and set it to the address of the load balancer.

   For example, if users type **`https://view.example.com`** in a browser to reach any of the load-balanced Connection Servers, add `balancedHost=view.example.com` to the `locked.properties` file.

3. Save the `locked.properties` file.

4. Restart the Connection Server service to make your changes take effect.

Allow HTML Access Through a Gateway

Connection Server instances that are directly behind a gateway, such as Unified Access Gateway, must know the address by which browsers will connect to the gateway when users use HTML Access.

For Connection Server instances that are behind a load-balancer or load-balanced gateway, perform the procedure described in Allow HTML Access Through a Load Balancer.

You must perform this procedure for each Connection Server that is behind the gateway.

Procedure

1. Create or edit the `locked.properties` file in the gateway configuration folder on the Connection Server host.

   For example: *`install_directory`*`\VMware\VMware View\Server\sslgateway\conf\locked.properties`

2 Add the `portalHost` property and set it to the address of the gateway.

   For example, if `https://view-gateway.example.com` is the address that browsers use to access VMware Horizon 8 through the gateway, add `portalHost=view-gateway.example.com` to the `locked.properties` file.

   If the Connection Server instance is behind multiple gateways, you can specify each gateway by adding a number to the `portalHost` property, for example:

```
portalHost.1=view-gateway-1.example.com
portalHost.2=view-gateway-2.example.com
```

   You must also specify multiple `portalHost` properties if a single gateway machine is known by more than one name.

3 Save the `locked.properties` file.

4 Restart the Connection Server service to make your changes take effect.

Configure the VMware Horizon 8 Web Portal Page for End Users

You can configure the VMware Horizon 8 web portal page to show or hide the icon for downloading Horizon Client, the icon for connecting to a remote desktop through HTML Access, and other links.

By default, the VMware Horizon 8 web portal page shows both an icon for downloading and installing Horizon Client, an icon for connecting through HTML Access, and a link pointing to the client download page on the VMware website. You can remove one or both of the icons from the VMware Horizon 8 web portal page by modifying the values in the `portal-links-html-access.properties` file.

Sometimes, you might want the links on the VMware Horizon 8 web portal page to point to an internal web server, or you might want to make specific client versions available on your own server. You can reconfigure the VMware Horizon 8 web portal page to point to a different download URL by modifying the contents of the `portal-links-html-access.properties` file. If that file is unavailable or is empty, and the `oslinks.properties` file exists, the `oslinks.properties` file determines the link value for the installer file.

You can define installer links for specific client operating systems in the `portal-links-html-access.properties` file or the `oslinks.properties` file. For example, if you browse to the VMware Horizon 8 web portal page from a macOS system, the link for the Horizon Client for Mac installer appears. For Linux clients, you can make separate links for 32-bit and 64-bit installers. For Chrome clients, you can substitute the link to Horizon Client for Chrome in the Chrome Web Store (https://chrome.google.com/webstore/detail/vmware-horizon-client-for/ppkfnjlimknmjoaemnpidmdlfchhehel).

Procedure

1 On the Connection Server host, use a text editor to open the `portal-links-html-access.properties` file in the *`CommonAppDataFolder`*`\VMware\VDM\portal\portal-links-html-access.properties` directory.

The *CommonAppDataFolder* directory is usually in the `C:\ProgramData` directory. To show the `C:\ProgramData` folder in Windows Explorer, use the Folder Options dialog box to show hidden folders.

Note If the `portal-links-html-access.properties` file does not exist, you can use the `oslinks.properties` file to modify the URLs used for downloading specific installer files. See the next step of this procedure.

2 Edit the configuration properties.

By default, both the installer icon and the HTML Access icon are enabled and a link points to the client download page on the VMware website. To deactivate an icon, which removes the icon from the web page, set the property to `false`.

Option	Property Setting
Disable HTML Access	`enable.webclient=false` Setting this option to false removes the HTML Access icon from the VMware Horizon 8 web portal page. ■ If this option is set to false, but the `enable.download` option is set to true, the user is taken to a web page for downloading the native Horizon Client installer. ■ If both options are set to false, the user sees the following message: `"Contact your local administrator for instructions on accessing this Connection Server."`
Disable downloading Horizon Client	`enable.download=false` Setting this option to false removes the Horizon Client download icon from the VMware Horizon web portal page. ■ If this option is set to false, but the `enable.webclient` option is set to true, the user is taken to the HTML Access login web page. ■ If both options are set to false, the user sees the following message: `"Contact your local administrator for instructions on accessing this Connection Server."`
Change the URL of the Web page for downloading Horizon Client	`link.download=https://`*`url-of-web-server`* Use this property if you plan to create your own web page.

Option	Property Setting

Create links for specific installers	The following examples show full URLs. If you place the installer files in the `downloads` directory, which is under the `C:\Program Files\VMware\VMware View\Server\broker\webapps\` directory on the Connection Server host, you can use relative URLs as described in a later step of this procedure.
	■ General link to download installer:
	`link.download=https://server/downloads`
	■ 64-bit Windows installer:
	`link.win64=https://server/downloads/VMware-Horizon-Client-x86_64-build#.exe`
	■ 64-bit Linux installer:
	`link.linux64=https://server/downloads/VMware-Horizon-Client-build#.x64.bundle`
	■ macOS installer:
	`link.mac=https://server/downloads/VMware-Horizon-Client-build#.dmg`
	■ iOS installer:
	`link.ios=https://server/downloads/VMware-Horizon-Client-iPhoneOS-build#.ipa`
	■ Android installer:
	`link.android=https://server/downloads/VMware-Horizon-Client-AndroidOS-build#.apk`

Change the URL for the Help link in the login page	`link.help` By default, this link points to a help system hosted on the VMware website. The Help link appears at the bottom of the login page.

3 (Optional) If the `portal-links-html-access.properties` file does not exist, use the `oslinks.properties` file to modify the URLs used for downloading specific installer files.

Note The `oslinks.properties` file can be used only to configure the links to specific installer files. If this file is missing during the HTML Access session, the download link directs users to `https://www.vmware.com/go/viewclients` by default.

a On the Connection Server host, use a text editor to open the `oslinks.properties` file in the *<installation-directory>*`\VMware\VMware View\Server\broker\webapps\portal\WEB-INF` directory.

b Configure the URLs for downloading specific installer files.

If you place the installer files in the `downloads` directory, which is under the `C:\Program Files\VMware\VMware View\Server\broker\webapps\` directory on the Connection Server host, you can use relative URLs as described in the next step of this procedure.

The `oslinks.properties` file contains the following default values.

```
link.download=https://www.vmware.com/go/viewclients
# download Links for particular platforms
link.win64=https://www.vmware.com/go/viewclients#win64
link.linux64=https://www.vmware.com/go/viewclients#linux64
link.mac=https://www.vmware.com/go/viewclients#mac
link.ios=https://itunes.apple.com/us/app/vmware-view-for-ipad/id417993697
link.android=https://play.google.com/store/apps/details?
id=com.vmware.view.client.android
```

4 To have users download installers from a location other than the VMware website, place the installer files on the HTTP server where the installer files reside.

This location must correspond to the URLs that you specified in the `portal-links-html-access.properties` file or in the `oslinks.properties` file from the previous steps. For example, to place the files in a `downloads` directory on the Connection Server host, use the following path.

```
C:\Program Files\VMware\VMware View\Server\broker\webapps\downloads
```

The links to the installer files can then use relative URLs with the format `/downloads/`*`client-installer-file-name`*.

5 Restart the Horizon Web Component service.

Replacing Default Ports for VMware Horizon 8 Services

During installation, VMware Horizon 8 services are set up to listen on certain network ports by default. In certain organizations, these ports must be changed to comply with organization policies

or to avoid contention. You can change the default ports that are used by Connection Server and PCoIP Secure Gateway.

Changing ports is an optional setup task. Use the default ports if your deployment does not require you to change them.

For a list of the default TCP and UDP ports that are used by VMware Horizon 8 servers, see the *Horizon Security* document.

Replace the Default HTTP Ports or NICs for Horizon Connection Server Instances

You can replace the default HTTP ports or NICs for a Connection Server instance by editing the `locked.properties` file on the server computer. Your organization might require you to perform these tasks to comply with organization policies or to avoid contention.

The default SSL port is 443. The default non-SSL port is 80.

The port that is specified in the secure tunnel External URL does not change as a result of changes that you make to ports in this procedure. Depending on your network configuration, you might have to change the secure tunnel External URL port as well.

If the server computer has multiple NICs, the computer listens on all NICs by default. You can select one NIC to listen on the configured port by specifying the IP address that is bound to that NIC.

During installation, VMware Horizon 8 configures the Windows firewall to open the required default ports. If you change a port number or the NIC on which it listens, you must manually reconfigure your Windows firewall to open the updated ports so that client devices can connect to the server.

If you change the SSL port number and you need HTTP redirection to continue working, you must also change the port number for HTTP redirection. See Change the Port Number for HTTP Redirection to Connection Server.

Prerequisites

Verify that the port that is specified in the External URL for this Connection Server instance will continue to be valid after you change ports in this procedure.

Procedure

1 Create or edit the `locked.properties` file in the gateway configuration folder on the Connection Server computer.

   For example: *`install_directory`*`\VMware\VMware View\Server\sslgateway\conf\locked.properties`

   The properties in the `locked.properties` file are case sensitive.

2 Add the `serverPort` or `serverPortNonSsl` property, or both properties, to the `locked.properties` file.

   For example:

```
serverPort=4443
serverPortNonSsl=8080
```

3 (Optional) If the server computer has multiple NICs, select one NIC to listen on the configured ports.

   Add the `serverHost` and `serverHostNonSsl` properties to specify the IP address that is bound to the designated NIC.

   For example:

```
serverHost=10.20.30.40
serverHostNonSsl=10.20.30.40
```

   Typically, both the SSL and non-SSL listeners are configured to use the same NIC. However, if you use the `serverProtocol=http` property to off-load SSL for client connections, you can set the `serverHost` property to a separate NIC to provide SSL connections to systems that are used to launch Horizon Console.

   If you configure SSL and non-SSL connections to use the same NIC, the SSL and non-SSL ports must not be the same.

4 Restart the Connection Server service to make your changes take effect.

What to do next

If necessary, manually configure your Windows firewall to open the updated ports.

Replace the Default Ports or NICs for the PCoIP Secure Gateway on Horizon Connection Server Instances

You can replace the default ports or NICs that are used by a PCoIP Secure Gateway service that runs on a Connection Server instance. Your organization might require you to perform these tasks to comply with organization policies or to avoid contention.

For client-facing TCP and UDP connections, the PCoIP Secure Gateway listens on port 4172 by default. For UDP connections to remote desktops, the PCoIP Secure Gateway listens on port 55000 by default.

The port that is specified in the PCoIP External URL does not change as a result of changes that you make to ports in this procedure. Depending on your network configuration, you might have to change the PCoIP External URL port as well.

If the computer on which the PCoIP Secure Gateway is running has multiple NICs, the computer listens on all NICs by default. You can select one NIC to listen on the configured ports by specifying the IP address that is bound to that NIC.

Prerequisites

Verify that the port that is specified in the PCoIP External URL on the Connection Server instance will continue to be valid after you change ports in this procedure.

Procedure

1. Start the Windows Registry Editor on the Connection Server computer where the PCoIP Secure Gateway is running.
2. Navigate to the `HKEY_LOCAL_MACHINE\SOFTWARE\Teradici\SecurityGateway` registry key.
3. Under this registry key, add one or more of the following String (`REG_SZ`) values with your updated port numbers.

   For example:

   ```
   ExternalTCPPort "44172"
   ExternalUDPPort "44172"
   InternalUDPPort "55111"
   ```

4. (Optional) If the computer on which the PCoIP Secure Gateway is running has multiple NICs, select one NIC to listen on the configured ports.

   Under the same registry key, add the following String (`REG_SZ`) values to specify the IP address that is bound to the designated NIC.

   For example:

   ```
   ExternalBindIP "10.20.30.40"
   InternalBindIP "172.16.17.18"
   ```

   If you configure external and internal connections to use the same NIC, the external and internal UDP ports must not be the same.
5. To make your changes take effect, restart the VMware Horizon PCoIP Secure Gateway service.

Replace the Default Control Port for PCoIP Secure Gateway on Connection Server Instances

You can replace the default port that controls the PCoIP Secure Gateway (PSG) service that runs on a Connection Server instance. You might need to perform this task to avoid port contention.

The PCoIP Secure Gateway listens for control connections on the local TCP port 50060 by default.

Procedure

1. Create or edit the `locked.properties` file in the gateway configuration folder on the Connection Server computer where the PCoIP Secure Gateway is running.

   For example: *`install_directory`*`\VMware\VMware View\Server\sslgateway\conf\locked.properties`

   The properties in the `locked.properties` file are case sensitive.

2 Add the `psgControlPort` property to the `locked.properties` file.

For example:

```
psgControlPort=52060
```

3 Start the Windows Registry Editor on the same machine.

4 Navigate to the `HKEY_LOCAL_MACHINE\SOFTWARE\Teradici\SecurityGateway` registry key.

5 Under this registry key, add the following String (`REG_SZ`) value with your updated port number.

For example:

```
TCPControlPort "52060"
```

Note The port number for `TCPControl Port` is the same as the port number for `psgControlPort`.

6 Restart the Connection Server service to make your changes take effect.

Change the Port Number for HTTP Redirection to Connection Server

If you replace the default port 443 on a Connection Server, and you want to allow HTTP redirection for Horizon Clients that attempt to connect to port 80, you must configure the `locked.properties` file on the Connection Server.

Note This procedure has no effect if you off-load SSL to an intermediate device. With SSL off-loading in place, the HTTP port on the Connection Server provides service to clients.

Prerequisites

Verify that you changed the default port number from 443. If you use the default values that are configured during installation, you do not have to perform this procedure to preserve the HTTP redirection rule.

Procedure

1 Create or edit the `locked.properties` file in the gateway configuration folder on the Connection Server computer.

For example: *`install_directory`*`\VMware\VMware View\Server\sslgateway\conf\locked.properties`

The properties in the `locked.properties` file are case sensitive.

2 Add the following lines to the `locked.properties` file:

```
frontMappingHttpDisabled.1=5:*:moved:https::port
frontMappingHttpDisabled.2=3:/error/*:file:docroot
frontMappingHttpDisabled.3=1:/admin*:missing
frontMappingHttpDisabled.4=1:/view-vlsi*:missing
```

In the preceding lines, the variable *port* is the port number to which the client should connect.

If you do not add the preceding lines, the *port* remains 443.

3 Restart the Connection Server service to make your changes take effect.

Prevent HTTP Redirection for Client Connections to Connection Server

Attempts by Horizon Clients to connect to Connection Servers over HTTP are silently redirected to HTTPS. In some deployments, you might want to prevent users from entering **`http://`** in their Web browsers and force them to use HTTPS. To prevent HTTP redirection for Horizon Clients, you must configure the `locked.properties` file on the Connection Server.

Note This procedure has no effect if you off-load SSL to an intermediate device. With SSL off-loading in place, the HTTP port on the Connection Server provides service to clients.

Procedure

1 Create or edit the `locked.properties` file in the gateway configuration folder on the Connection Server computer.

For example: *`install_directory`*`\VMware\VMware View\Server\sslgateway\conf\locked.properties`

The properties in the `locked.properties` file are case sensitive.

2 Add the following lines to the `locked.properties` file:

```
frontMappingHttpDisabled.1=5:*:missing
frontMappingHttpDisabled.2=3:/error/*:file:docroot
```

3 Restart the Connection Server service to make your changes take effect.

Enable Remote Access to VMware Horizon 8 Performance Counters on Connection Servers

VMware Horizon 8 performance counters are available locally on a Connection Server but return 0 when accessed from another computer. To enable remote access to VMware Horizon 8 performance counters on Connection Servers, you must configure Connection Server's framework port in the registry.

Procedure

1 Start the Windows Registry Editor.

2 Navigate to the `HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.\VMware VDM\Node Manager` registry key.

3 Add a new String (REG_SZ) value, `Management Port`.

4 Set the `Management Port` value to **32111**.

Sizing Windows Server Settings to Support Your Deployment

To support a large deployment of remote desktops, you can configure the Windows Server computers on which you install Connection Server. On each computer, you can size the Windows page-file.

On Windows Server 2012 R2 and later computers, the ephemeral ports, TCB hash table, and Java Virtual Machine settings are sized by default. These adjustments ensure that the computers have adequate resources to run correctly with the expected user load.

Sizing Memory for Horizon Connection Server

On a Connection Server computer, 10GB of memory is required for deployments of 50 or more remote desktops. A Windows Server computer with at least 10GB of memory is automatically configured to support approximately 2,000 concurrent tunnel sessions, the maximum number that Connection Server can support.

Configure less than 10GB of memory for small, proof-of-concept deployments only. With the required minimum of 4GB of memory, a configuration can support approximately 500 concurrent tunnel sessions, which is more than adequate to support small, proof-of-concept deployments.

However, because your deployment might grow larger as more users are added to the environment, VMware recommends that you always configure at least 10GB of memory. Make an exception only when you know that the environment will not grow, and memory is not available.

If you install Connection Server with less than 10GB of memory, VMware Horizon 8 provides memory recommendations by generating warning messages after the installation is complete. An event triggered every 12 hours states that the Connection Server instance is configured with a small amount of physical memory.

If you increase a computer's memory to 10GB to support a larger deployment, restart Connection Server to ensure that the JVM heap size is automatically increased to the recommended value. You do not have to reinstall Connection Server.

Important Do not change the JVM heap size on 64-bit Windows Server computers. Changing this value might make Connection Server behavior unstable. On 64-bit computers, the Connection Server service sets the JVM heap size to accord with the physical memory.

For additional hardware and memory requirements for Connection Server, see Hardware Requirements for Horizon Connection Server - Install and Upgrade.

For hardware and memory recommendations for using Connection Server in a large deployment, see "Connection Server Maximums and Virtual Machine Configuration" in the *Horizon Overview and Deployment Planning* document.

Configure the System Page-File Settings

You can optimize the virtual memory on the Windows Server computers on which your Connection Server instances are installed by changing the system page-file settings.

When Windows Server is installed, Windows calculates an initial and maximum page-file size based on the physical memory installed on the computer. These default settings remain fixed even after you restart the computer.

If the Windows Server computer is a virtual machine, you can change the memory size through vCenter Server. However, if Windows uses the default setting, the system page-file size does not adjust to the new memory size.

Procedure

1. On the Windows Server computer on which Connection Server is installed, navigate to the Virtual Memory dialog box.

   By default, **Custom size** is selected. An initial and maximum page-file size appear.

2. Click **System managed size**.

Results

Windows continually recalculates the system page-file size based on current memory use and available memory.

Deploying VMware Horizon 8 on VMware Cloud on AWS

7

VMware Cloud on AWS is a VMware SDDC infrastructure-as-a-service on AWS where you can deploy VMware Horizon 8 desktops and applications.

You can select AWS as an available deployment type when you install Connection Server. You can also provide AWS as a deployment type during a silent installation of Connection Server. Once you select AWS as a deployment type, Horizon will automatically operate in a mode that is compatible with the VMware Cloud on AWS cloud admin privileges. For more information about deploying VMware Horizon on VMware Cloud on AWS, see Architectural Overview section of the reference architecture at https://techzone.vmware.com/resource/horizon-on-vmware-cloud-on-aws-architecture#architectural-overview.

For a list of VMware Horizon 8 features supported on VMware Cloud on AWS, see the VMware Knowledge Base article https://kb.vmware.com/s/article/58539.

For more information about VMware Cloud on AWS, see the VMware Cloud on AWS documentation at https://docs.vmware.com/en/VMware-Cloud-on-AWS/index.html.

For more information about the impact of SDDC upgrade on a VMware Horizon 8 deployment on VMware Cloud on AWS, see the VMware Knowledge Base article https://kb.vmware.com/s/article/74599.

For more information about updating the vSAN Storage Policy FTT Level on a VMware Horizon 8 deployment on VMware Cloud on AWS, see the VMware Knowledge Base article https://kb.vmware.com/s/article/76366.

For more information on connecting your VMware Horizon 8 on VMware Cloud on AWS deployment with the Horizon Control Plane and getting a subscription license, see "Enabling VMware Horizon 8 for Subscription Licenses and Horizon Control Plane Services" in the *Horizon Administration* document.

Deploying Horizon on Google Cloud VMware Engine

Google Cloud VMware Engine (GCVE) is a VMware SDDC infrastructure-as-a-service on Google Cloud where you can deploy VMware Horizon desktops and applications. Check with your Google Cloud representative on the availability of GCVE.

You can select Google Cloud as an available deployment type when you install Connection Server. You can also provide Google Cloud as a deployment type during a silent installation of Connection Server.

For more information about deploying Horizon on GCVE, please see reference architecture at https://techzone.vmware.com/resource/horizon-on-google-cloud-vmware-engine-architecture. For the latest information on support, please see Knowledge Base article 81922.

Deploying VMware Horizon 8 on Azure VMware Solution

8

Azure VMware Solution (AVS) is a VMware SDDC infrastructure-as-a-service on Microsoft Azure where you can deploy VMware Horizon 8 desktops and applications. Check with your Microsoft representative on the availability of AVS.

You can select Azure as an available deployment type when you install Connection Server. You can also provide Azure as a deployment type during a silent installation of Connection Server. Once you select Azure as a deployment type, Horizon will automatically operate in a mode that is compatible with the Azure VMware Solution cloud admin privileges.

You can create instant-clone and full-clone desktop pools on AVS.

For the Horizon on Azure VMware Solution reference architecture, please see the Horizon 8 on Azure VMware Solution Architecture. For the latest Horizon support information for Azure VMware Solution, please see Knowledge Base article 80850.

Deploying VMware Horizon 8 on Native Amazon EC2

9

You can deploy Windows Remote Desktop Services (RDS) hosts on native Amazon EC2 to support manual farms.

You start out by configuring an AWS account and creating an EC2 instance type and quantity based on your requirement. You then deploy the VMware Horizon 8 server components on the Amazon EC2 machines. You can also deploy additional components as required such as events database, Active Directory domain controllers, or file shares.

For more information on creating manual farms, see Creating and Managing Farms in the *Windows Desktops and Applications in Horizon* document.

Deploying VMware HorizonVMware Horizon 8 on Amazon Workspaces

10

You can create manual desktop pools to support VDI use cases on Amazon Workspaces.

For more information, see Creating and Managing Manual Desktop Pools in the *Windows Desktops and Applications in Horizon* document.

Deploying VMware Horizon 8 on VMware Cloud on Dell EMC

11

Deploying VMware Horizon 8 on VMware Cloud on Dell EMC provides a platform to host VMware Horizon 8 desktops in an on-premises managed infrastructure.

For more information about deploying VMware Horizon 8 on VMware Cloud on Dell EMC, see the *VMware Cloud on Dell EMC Horizon Integration* guide available at https://docs.vmware.com/en/VMware-Cloud-on-Dell-EMC/index.html.

Configuring Event Reporting in Horizon Console

12

You can create an event database to record information about VMware Horizon 8events. In addition, if you use a Syslog server, you can configure Connection Server to send events to a Syslog server or create a flat file of events written in `Syslog` format.

This chapter includes the following topics:

Add a Database and Database User for VMware Horizon 8 Events in Horizon Console

You create an event database by adding it to an existing database server. You can then use reporting software to analyze the events in the database.

Deploy the database server for the event database on a dedicated server, so that event logging activity does not affect provisioning and other activities that are critical for VMware Horizon 8 deployments.

Note You do not need to create an ODBC data source for this database.

Prerequisites

- Verify that you have a supported Microsoft SQL Server, Oracle, or PostgreSQL database server on a system that a Connection Server instance has access to.

  For the most up-to-date information about supported databases, see the VMware Product Interoperability Matrixes at http://www.vmware.com/resources/compatibility/sim/interop_matrix.php. For **Solution/Database Interoperability**, after you select the product and version, for the Add Database step, to see a list of all supported databases, select **Any** and click **Add**.

- Verify that you have the required database privileges to create a database and user on the database server.

Procedure

1. Add a database to the server and give it a descriptive name such as HorizonEvents.

   For an Oracle 12c or Oracle 11g database, also provide an Oracle System Identifier (SID), which you use when you configure the event database in Horizon Console.

2. Add a user for this database that has permission to create tables, views, and, Oracle triggers and sequences, and permission to read from and write to these objects.

   For a Microsoft SQL Server database, VMware Horizon 8 does not support the Integrated Windows Authentication security model method of authentication. Use the SQL Server Authentication method of authentication, which is the only supported method.

Results

The database is created, but the schema is not installed until you configure the database in Horizon Console.

What to do next

Follow the instructions in Configure the Event Database in Horizon Console.

Prepare an SQL Server Database for Event Reporting in Horizon Console

Before you can use Horizon Console to configure an event database on Microsoft SQL Server, you must configure the correct TCP/IP properties and verify that the server uses SQL Server Authentication.

Prerequisites

- Create an SQL Server database for event reporting. See Add a Database and Database User for VMware Horizon 8 Events in Horizon Console.
- Verify that you have the required database privileges to configure the database.
- Verify that the database server uses the SQL Server Authentication method of authentication. Do not use Windows Authentication.

Procedure

1. Open SQL Server Configuration Manager and expand **SQL Server *YYYY* Network Configuration**.
2. Select **Protocols for *server_name***.
3. In the list of protocols, right-click **TCP/IP** and select **Properties.**
4. Set the **Enabled** property to **Yes.**

5 Verify that a port is assigned or, if necessary, assign one.

For information on the static and dynamic ports and how to assign them, see the online help for the SQL Server Configuration manager.

6 Verify that this port is not blocked by a firewall.

What to do next

Use Horizon Console to connect the database to Connection Server. Follow the instructions in Configure the Event Database in Horizon Console.

Prepare a PostgreSQL Database for Event Reporting in Horizon Console

Before you can use Horizon Console to configure an event database on PostgreSQL, you must edit a configuration file so that the Connection Server can communicate with the PostgreSQL database.

Prerequisites

- Create a PostgreSQL database for event reporting. See Add a Database and Database User for VMware Horizon 8 Events in Horizon Console.
- Verify that you have the required database privileges to configure the database.

Procedure

1 In the directory where PostgreSQL is installed, open the `data/pg_hba` file for editing.

2 Add the following row to the table under `IPv4 local connections` (replace *<IP address of Connection Server>* with the actual IP address of the Connection Server):

TYPE	DATABASE	USER	ADDRESS	METHOD
host	all	all	<IP address of Connection Server>	md5

3 Save the file.

What to do next

Use Horizon Console to connect the database to Connection Server. Follow the instructions in Configure the Event Database in Horizon Console.

Configure the Event Database in Horizon Console

The event database stores information about VMware Horizon 8 events as records in a database rather than in a log file.

You configure an event database after installing a Connection Server instance. You need to configure only one host in a Connection Server group. The remaining hosts in the group are configured automatically.

Note The security of the database connection between the Connection Server instance and an external database is the responsibility of the administrator, although event traffic is limited to information about the health of the VMware Horizon 8 environment.

- If you want to take extra precautions, you can secure this channel through IPSec or other means, or you can deploy the database locally on the Connection Server computer.
- By default Connection Server connects to the event database in non-SSL mode. For information about enabling SSL connection, see SSL Connection to Event Database.

You can use Microsoft SQL Server, Oracle, or PostgreSQL database reporting tools to examine events in the database tables. For more information, see the *Horizon Administration* document.

You can also generate VMware Horizon 8 events in `Syslog` format so that the event data can be accessible to third-party analytics software. You use the `vdmadmin` command with the `-I` option to record VMware Horizon 8 event messages in `Syslog` format in event log files. See "Generating VMware Horizon 8 Event Log Messages in Syslog Format Using the -I Option" in the *Horizon Administration* document.

Prerequisites

You need the following information to configure an event database:

- The DNS name or IP address of the database server.
- The type of database server: Microsoft SQL Server, Oracle, or PostgreSQL.
- The port number that is used to access the database server. The default is 1521 for Oracle and 1433 for SQL Server. For SQL Server, if the database server is a named instance or if you use SQL Server Express, you might need to determine the port number. See the Microsoft KB article about connecting to a named instance of SQL Server, at http://support.microsoft.com/kb/265808.
- The name of the event database that you created on the database server. See Add a Database and Database User for VMware Horizon 8 Events in Horizon Console.

  For an Oracle 12c or 11g database, you must use the Oracle System Identifier (SID) as the database name when you configure the event database in Horizon Console.
- The username and password of the user you created for this database. See Add a Database and Database User for VMware Horizon 8 Events in Horizon Console.

  For SQL Server, use SQL Server Authentication for this user. Do not use the Integrated Windows Authentication security model method of authentication.

- A prefix for the tables in the event database, for example, VE_. The prefix enables the database to be shared among VMware Horizon 8 installations.

  Note You must enter characters that are valid for the database software you are using. The syntax of the prefix is not checked when you complete the dialog box. If you enter characters that are not valid for the database software you are using, an error occurs when Connection Server attempts to connect to the database server. The log file indicates all errors, including this error and any others returned from the database server if the database name is invalid.

Procedure

1 In Horizon Console, select **Settings > Event Configuration**.

2 In the **Event Database** section, click **Edit**, enter the information in the fields provided, and click **OK**.

  To clear the event database information, click **Clear**.

3 (Optional) In the Event Settings window, click **Edit**, change the length of time to show events and the number of days to classify events as new, and click **OK**.

  These settings pertain to the length of time the events are listed in the Horizon Console interface. After this time, the events are only available in the historical database tables.

  Note Timing profiler data is removed from all database tables, so it is not available in historical tables.

  Commands for activating and deactivating the timing profiler are as follows.

  - To activate the timing profiler on a Connection Server instance that does not use a management port:

    ```
    vdmadmin -I -timingProfiler -enable
    ```

  - To activate the timing profiler on a Connection Server instance that uses a management port:

    ```
    vdmadmin -I -timingProfiler -enable -server {ip/server}
    ```

  - To deactivate the timing profiler on a Connection Server instance:

    ```
    vdmadmin -I -timingProfiler -disable
    ```

4 Select **Monitoring > Events** to verify that the connection to the event database is successful.

  If the connection is unsuccessful, an error message appears. If you are using SQL Express or if you are using a named instance of SQL Server, you might need to determine the correct port number, as mentioned in the prerequisites.

SSL Connection to Event Database

By default Connection Server connects to the event database in non-SSL mode. You can switch between non-SSL and SSL modes using the steps below.

Switch to SSL Connection Mode

1 Confirm that the database can accept SSL connections.

2 Confirm that the database certificate is trusted by the Windows machine containing the connection server. If it is not, you can remedy this by importing the database certificate to the machine and adding it to the Windows trust store.

3 Under **Local Ldap > OU=Properties > OU=Global > CN=Common**, set the `pae-enableDbSSL` flag to `1`.

4 Restart the connection server.

All database connections are now created using SSL. If the database does not support SSL or the database certificates are not trusted by the Windows machine containing the connection server, the database connections will fail.

Switch Back to Non-SSL Connection Mode

1 Under **Local Ldap > OU=Properties > OU=Global > CN=Common**, set the `pae-enableDbSSL` flag to `0`.

2 Restart the connection server.

Configure Event Logging to File or Syslog Server in VMware Horizon 8

You can generate VMware Horizon 8 events in `Syslog` format so that the event data can be accessible to analytics software.

You need to configure only one host in a Connection Server group. The remaining hosts in the group are configured automatically.

If you enable file-based logging of events, events are accumulated in a local log file. If you specify a file share, these log files are moved to that share.

- The maximum size of the local directory for event logs, including closed log files, before the oldest files are deleted, is 300MB. The default destination of the Syslog output is `%PROGRAMDATA%\VMware\VDM\events\`.
- Use a UNC path to save log files for a long-term record of events, or if you do not have a Syslog server or event database, or if your current Syslog server does not meet your needs.

You can alternatively use a `vdmadmin` command to configure file-based logging of events in Syslog format. See the topic about generating VMware Horizon 8 event log messages in Syslog format using the `-I` option of the `vdmadmin` command, in the *Horizon Administration* document.

Important When sending to a Syslog server, Syslog data is sent across the network without software-based encryption, and might contain sensitive data, such as user names. VMware recommends using link-layer security, such as IPSEC, to avoid the possibility of this data being monitored on the network.

Prerequisites

You need the following information to configure Connection Server so that events can be recorded in Syslog format or sent to a Syslog server, or both:

- If you plan to use a Syslog server to listen for the VMware Horizon 8 events on a UDP port, you must have the DNS name or IP address of the Syslog server and the UDP port number. The default UDP port number is 514.
- If you plan to collect logs in a flat-file format, you must have the UNC path to the file share and folder in which to store the log files, and you must have the user name, domain name, and password of an account that has permission to write to the file share.

Procedure

1. In VMware Horizon 8, select **Settings > Event Configuration**.
2. (Optional) In the **Syslog** area, to configure Connection Server to send events to a Syslog server, click **Add** below **Send to syslog servers**, and supply the server name or IP address and the UDP port number.
3. (Optional) In the **Events to File System** area, choose whether or not to enable event log messages to be generated and stored in Syslog format in log files.

Option	Description
Always	Always generate and store event log messages in Syslog format in log files.
Log to file on error (default)	Log audit events to a log file when there is a problem writing events to the event database or the Syslog server. This option is enabled by default.
Never	Never generate and store event log messages in Syslog format in log files.

   The log files are retained locally unless you specify a UNC path to a file share.

4. (Optional) To store the VMware Horizon 8 event log messages on a file share, click **Add** below **Copy to location**, and supply the UNC path to the file share and folder in which to store the log files, along with the user name, domain name, and password of an account that has permission to write to the file share.

   An example of a UNC path is:

```
\\syslog-server\folder\file
```

Installing VMware Horizon 8 in an IPv6 or Mixed IPv4/IPv6 Environment

13

VMware Horizon 8 supports IPv6 as an alternative to IPv4. A Horizon pod must be either IPv6 only or IPv4 only. However, connections from both IPv4 and IPv6 client devices to the same Horizon pod are supported through Unified Access Gateway.

See the Unified Access Gateway documentation for information on how to configure Unified Access Gateway to support a mixed IPv4/IPv6 environment.

Not all VMware Horizon 8 features that are supported in an IPv4 environment are supported in an IPv6 or mixed environment. VMware Horizon 8 does not support upgrading from an IPv4 environment to an IPv6 environment. Also, VMware Horizon 8 does not support migration between IPv4 and IPv6 environments.

Important To run VMware Horizon 8 in an IPv6 environment, you must specify IPv6 when you install all VMware Horizon 8 components.

Setting Up VMware Horizon 8 in an IPv6 Environment

To run VMware Horizon 8 in an IPv6 environment, you must be aware of the requirements and choices that are specific to IPv6 when you perform certain administrative tasks.

Before you install VMware Horizon 8, you must have a working IPv6 environment. The following VMware Horizon 8 administrative tasks have options that are specific to IPv6.

- Installing Horizon Connection Server. See Install Horizon Connection Server with a New Configuration.
- Installing View Replica Server. See Install a Replicated Instance of Horizon Connection Server.
- Configuring the PCoIP External URL. See Configure the Secure Tunnel and PCoIP Secure Gateway.
- Setting the PCoIP External URL. See Set the External URLs for Horizon Connection Server Instances.
- Modifying the PCoIP External URL. See Set the External URLs for Horizon Connection Server Instances.
- Installing Horizon Agent for Windows. See the Horizon Agent installation topics in the *Windows Desktops and Applications in Horizon* document.

- Installing Horizon Agent for Linux. See the Horizon Agent installation topics in the *Linux Desktops and Applications in Horizon* document.
- Installing Horizon Client. See Supported Clients in an IPv6 Environment.

Note VMware Horizon 8 does not require you to enter an IPv6 address in any administrative tasks. In cases where you can specify either a fully qualified domain name (FQDN) or an IPv6 address, it is highly recommended that you specify an FQDN to avoid potential errors.

Supported vSphere, Database, and Active Directory Versions in an IPv6 Environment

In an IPv6 environment, VMware Horizon 8 supports specific vSphere, database server, and Active Directory versions.

For the most up-to-date information about supported databases, vSphere versions, and Active Directory versions in an IPv6 environment, see the VMware Product Interoperability Matrixes at http://www.vmware.com/resources/compatibility/sim/interop_matrix.php.

Supported Operating Systems for VMware Horizon Servers in an IPv6 Environment

You must install VMware Horizon 8 servers on specific Windows Server operating systems.

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

Supported Windows Operating Systems for Desktops and RDS Hosts in an IPv6 Environment

VMware Horizon 8 supports specific Windows operating systems for desktop machines and RDS hosts. RDS hosts provide session-based desktops and applications to users.

Supported Linux Distributions for Desktops and Multi-Session Hosts in an IPv6 Environment

VMware Horizon 8 supports specific Linux distributions for desktop machines and multi-session hosts. Multi-session hosts provide session-based desktops and applications to users.

For more information, see the system requirements and multi-session topics in the *Linux Desktops and Applications in Horizon* document.

Supported Clients in an IPv6 Environment

In an IPv6 environment, VMware Horizon 8 supports clients that run on specific desktop operating systems.

- Windows 10 32-bit or 64-bit Home, Pro, Pro for Workstations, Enterprise, and IoT Enterprise are supported.
- On iOS devices, Horizon Client for iOS 4.1 or later is required.
- On macOS devices, Horizon Client for Mac 4.9 or later is required.
- On Android devices, Horizon Client for Android 4.9 or later is required.
- On Chromebook devices, Horizon Client for Android 5.1 or later is required.
- On Linux devices, Horizon Client for Linux 2006 or later is required.

The following clients are not supported.

- Horizon Client for Chrome
- Horizon Client for Windows 10 UWP
- PCoIP Zero Client

Supported Remoting Protocols in an IPv6 Environment

In an IPv6 environment, VMware Horizon 8 supports specific remoting protocols.

The following remoting protocols are supported:

- RDP
- RDP with Secure Tunnel
- PCoIP
- PCoIP through PCoIP Secure Gateway
- VMware Blast
- VMware Blast through Blast Secure Gateway
- Blast Extreme Adaptive Transport (BEAT)

Supported Authentication Types in an IPv6 Environment

In an IPv6 environment, VMware Horizon 8 supports specific authentication types.

The following authentication types are supported:

- Password authentication using Active Directory
- Smart Card
- Single Sign-On

The following authentication types are not supported:

- SecurID
- RADIUS
- SAML

Other Supported Features in an IPv6 Environment

The following features are supported:

- Application pools
- Applications that run on a desktop pool
- Audio-out
- Automated desktop pools of full virtual machines and instant clones
- Blast Extreme Adaptive Transport (BEAT)
- Browser Redirection
- Client Drive Redirection/File transfer
- Clipboard
- Customer Experience Improvement Program (CEIP)
- Disk space reclamation
- DPI sync
- Drag and Drop
- Events
- File association
- Geolocation Redirection
- Horizon Performance Tracker
- HTML5 Multimedia Redirection
- Instant-clone desktop pools
- LDAP backup
- Local IME
- Location-Based Printing (LBP)
- Manual desktop pools, including vCenter Server virtual machines, physical computers, and virtual machines not managed by vCenter Server
- Native NFS snapshots (VAAI)
- Real-Time Audio-Video (RTAV)

- Published desktop pools
- RDS Host 3D
- Role-based administration
- RTAV
- Scanner redirection
- SDO Sensor Redirection
- Seamless Windows
- Serial port redirection
- Session Collaboration
- Single Sign-on, including the Log in as current user feature
- Smart Card Redirection
- System health dashboard
- TSMMR and DShowMMR
- Unity touch
- UNC Path Redirection
- URL Content Redirection
- USB redirection
- View Storage Accelerator
- VMware audio
- VMware Integrated Printing
- VMware video
- VMware Virtualization Pack for Skype for Business (Windows only)
- vSAN
- HTML Access

The following features are not supported:

- Cloud Pod Architecture
- Horizon Cloud Connector
- Horizon Agent Direct-Connection Plug-In, for Linux desktops
- Log Insight
- Microsoft Lync
- Microsoft Teams
- PCoIP with published instant-clone desktop pools

- Smart policies based on IP ranges, for Linux desktops
- Syslog
- Teradici TERA host card
- Virtual Volumes
- Untrusted domains

Unified Access Gateway Support for IPv4 and IPv6 Dual Mode

You can use Unified Access Gateway to act as a bridge for VMware Horizon 8 Clients to connect to a back-end Horizon Connection Server or agent environment. In this scenario, Horizon Client and the Horizon Connection Server can be configured with different IP modes: IPv4 or IPv6 and conversely.

The VMware Horizon 8 back-end environment might consist of Connection Servers, agent desktops, or other server-side infrastructure.

Horizon Client and Horizon Connection Server can have the following IP modes in the VMware Horizon 8 infrastructure:

Horizon Client	Horizon Connection Server	Supported
IPv4	IPv4	Yes
IPv6	IPv4	Yes
IPv6	IPv6	Yes
IPv4	IPv6	Yes

Note When Horizon Client and Horizon Connection Server are configured with different IP modes (IPv4 or IPv6 and conversely), the **Connection Server IP mode**, a setting in the Unified Access Gateway Admin UI, can have one of the following values: same IP mode as the Horizon Connection Server or mixed mode `(IPv4+IPv6)`.

For example: Horizon Client is configured with IPv4 and Horizon Connection Server is configured with IPv6, then the **Connection Server IP mode** can have either `IPv6` or `IPv4+IPv6` (mixed mode) values.

For more information about the **Connection Server IP mode** setting, see the Unified Access Gateway documentation.

Installing VMware Horizon 8 in FIPS Mode

14

VMware Horizon 8 can perform cryptographic operations using FIPS (Federal Information Processing Standard) 140-2 compliant algorithms. You can enable the use of these algorithms by installing VMware Horizon 8 in FIPS mode.

VMware Horizon 8 does not support upgrading from a non-FIPS installation to a FIPS installation.

Note To ensure that VMware Horizon 8 runs in FIPS mode, you must enable FIPS when you install all VMware Horizon 8 components.

This chapter includes the following topics:

Overview of Setting Up VMware Horizon 8 in FIPS Mode

To set up VMware Horizon 8 in FIPS mode, you must first enable FIPS mode in the Windows environment. Then you install all the VMware Horizon 8 components in FIPS mode.

The option to install VMware Horizon 8 in FIPS mode is available only if FIPS mode is enabled in the Windows environment. For more information about enabling FIPS mode in Windows, see https://support.microsoft.com/en-us/kb/811833.

Note Horizon Console does not indicate whether VMware Horizon 8 is running in FIPS mode.

To install VMware Horizon 8 in FIPS mode, perform the following administrative tasks.

- When installing Connection Server, select the FIPS mode option. See Install Horizon Connection Server with a New Configuration.
- When installing a replica server, select the FIPS mode option. See Install a Replicated Instance of Horizon Connection Server.
- Disable weak ciphers for Horizon Agent machines. See Disable Weak Ciphers in SSL/TLS.
- When installing Horizon Agent, select the FIPS mode option. See the Horizon Agent installation topics in the *Windows Desktops and Applications in Horizon* document.

- For Windows clients, enable FIPS mode in the client operating system and select the FIPS mode option when installing Horizon Client for Windows. See the *Horizon Client for Windows Guide* document.
- For Linux clients, enable FIPS mode in the client operating system. See the *Horizon Client for Linux Guide* document.

System Requirements for FIPS Mode

To support FIPS mode, your VMware Horizon 8 deployment must meet the following requirements.

vSphere

- vCenter Server 6.5 or later
- ESXi 6.5 or later

Remote desktop

Windows desktops and Linux desktops can both support FIPS mode, after meeting the following requirements.

- Windows desktop
  - The desktop can run any Windows platform supported by Horizon Agent.
  - The Windows desktop must have a FIPS certificate. For information, see "FIPS 140 Validation" on the Microsoft TechNet website.
  - Horizon Agent must be installed with the FIPS mode option selected.
- Linux desktop
  - The desktop can run any Red Hat Enterprise Linux (RHEL) distribution supported by Horizon Agent.
  - Horizon Agent must be installed with the FIPS option enabled (`-f yes`).
  - Desktops running RHEL 8.x must have FIPS mode enabled at the Linux system level:

    ```
    fips-mode-setup --enable
    reboot
    ```

Horizon Client

- Windows clients must meet the following requirements:
  - FIPS mode is enabled at the operating system level and a FIPS certificate is installed. For information, see "FIPS 140 Validation" on the Microsoft TechNet website.
  - Horizon Client must be installed with the FIPS option selected. See the *Horizon Client for Windows Guide* document.

- Linux clients must have FIPS mode enabled at the operating system level. See the *Horizon Client for Linux Guide* document.

Cryptographic protocol

- TLSv1.2

Connection Server

- The option to install VMware Horizon 8 in FIPS mode is available only if FIPS mode is enabled in the Windows environment. For more information about enabling FIPS mode in Windows, see https://support.microsoft.com/en-us/kb/811833
- A new installation of Connection Server in FIPS mode requires a CA-signed certificate with friendly name `vdm` to be placed in the Windows certificate store. The installer checks for the presence of this certificate before proceeding with the installation. See Configure Horizon Connection Server to Use a New TLS Certificate for more information.

VMware Horizon 8 Upgrade Overview

15

Upgrading an enterprise VMware Horizon 8 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 8 you use in your deployment.

1. If you have features that are no longer supported in the latest version of VMware Horizon 8, you must uninstall some of these features before proceeding with the upgrade. See Chapter 16 Uninstalling No Longer Supported and Deprecated Features.
2. Upgrade the Horizon Client software that runs on end users' client devices. See Chapter 17 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 VMware Horizon 8 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 20 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 8 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 8 platform for their critical deployments.

For more information on the ESB and the Horizon 8 versions that have been designated an ESB, see VMware Knowledge Base article 86477.

Uninstalling No Longer Supported and Deprecated Features

16

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 8 2012 or 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 8 2012 or 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 8 2012 or later 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 8 2012 or 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 8 2012 or later, you must remove View Composer and delete all your linked-clone desktop pools and farms. See Remove View Composer from VMware Horizon 8.

This chapter includes the following topics:

- Uninstall JMP Server
- Remove View Composer from VMware Horizon 8

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 8 2006 or 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 uninstall steps, click **Uninstall** and follow the wizard.

Remove View Composer from VMware Horizon 8

You can remove the connection between VMware Horizon 8 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 VMware Horizon 8 all the linked-clone virtual machines created by View Composer. VMware Horizon 8 prevents you from removing View Composer if any associated linked clones still exist. After the connection to View Composer is disabled, VMware Horizon 8 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 VMware Horizon 8. 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 17

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/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 and Upgrade* 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 8 Server Upgrades

18

Hosts and virtual machines in a VMware Horizon 8 deployment must meet specific hardware and operating system requirements.

Upgrading VMware Horizon 8 Server Components

19

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 the new version of VMware Horizon 8, 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 the new version of VMware Horizon 8, you must back up 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 8 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/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 the new version of VMware Horizon 8, 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 license key for the new version. 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- Install and Upgrade and Hardware Requirements for Horizon Connection Server - Install and Upgrade.
- Familiarize yourself with the security-related requirements of VMware Horizon 8, 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 and Upgrade* 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 8 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 8 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 the new version of VMware Horizon 8 on the cluster.

- If any node is upgraded to the new version of VMware Horizon 8 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 the new version of VMware Horizon 8 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 8 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 *Cloud Pod Architecture in Horizon*.

Upgrading VMware Horizon Servers 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 and Upgrade* document.

Upgrade vCenter Server

Perform a vCenter Server upgrade as part of the same maintenance window during which you upgrade other VMware Horizon 8 server components. Before you upgrade vCenter Server, you must back up some VMware Horizon 8 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 8 server components, at your next maintenance window, continue with the VMware Horizon 8 upgrade.

- If you are also upgrading vSphere components, see Chapter 20 Upgrade ESXi Hosts and Their Virtual Machines.
- If you upgrading only VMware Horizon 8 components, see Upgrade Horizon Agent .

Accept the Thumbprint of a Default TLS Certificate

When you add vCenter Server instances to VMware Horizon 8, 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 Chapter 5 Configuring TLS Certificates for VMware Horizon 8 Servers.

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 8. 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 VMware Horizon 8 Group Policy Administrative Template Files

VMware Horizon 8 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 8 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.

The Horizon 8 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

20

Upgrading ESXi hosts and virtual machines is the most time-consuming aspect of this middle phase of a VMware Horizon 8 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 8 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

21

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 *Linux Desktops and Applications 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 *Windows Desktops and Applications 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 *Linux Desktops and Applications 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 20 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 *Windows Desktops and Applications 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 *Windows Desktops and Applications 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 7.0/8.0.

Prerequisites

- Complete the system requirements for VMware Horizon 8 upgrade.
- 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.

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 VMware Horizon 8 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 later, 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 - Install and Upgrade.
- Verify that the RDS Host role is installed in the operating system. See the procedure called "Install Remote Desktop Services" in the *Windows 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 *Windows 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 8 Environment

22

If you upgrade vSphere components separately from VMware Horizon 8 components, you must back up some Horizon 8 data and reinstall some Horizon 8 software.

Instead of performing an integrated upgrade of Horizon 8 and vSphere components, you can choose to first upgrade all Horizon 8 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 Horizon 8 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.

Upgrading Horizon 8 in FIPS Mode

23

Upgrading an enterprise VMware Horizon 8 deployment in FIPS mode 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 8 you use in your deployment.

1 If you have features that are no longer supported in the latest version of VMware Horizon 8, you must uninstall some of these features before proceeding with the upgrade. See Chapter 16 Uninstalling No Longer Supported and Deprecated Features.

2 Upgrade the Horizon Client software that runs on end users' client devices. See Chapter 17 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 VMware Horizon 8 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 20 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 8 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 8 platform for their critical deployments.

For more information on the ESB and the Horizon 8 versions that have been designated an ESB, see VMware Knowledge Base article 86477.