Horizon Architecture Planning

VMware Horizon 2203

vmware®

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

https://docs.vmware.com/

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

Contents

Horizon Architecture Planning

Horizon Architecture Planning provides an introduction to VMware Horizon™, including a description of its major features and deployment options and an overview of how the components are typically set up in a production environment.

This guide answers the following question:

- Does the product solve the problems you need it to solve?

Not all features and capabilities of VMware Horizon are available in all license editions. For a comparison of feature sets in each edition, see https://www.vmware.com/products/horizon.html.

To help you protect your installation, this guide also provides a discussion of security features.

Intended Audience

This information is intended for IT decision makers, architects, administrators, and others who need to familiarize themselves with the components and capabilities of this product. With this information, architects and planners can determine whether VMware Horizon satisfies the requirements of their enterprise for efficiently and securely delivering virtual desktops and applications to their end users.

Introduction to VMware Horizon

1

With VMware Horizon, IT departments can run remote desktops and applications in the data center and deliver these desktops and applications to employees. End users gain a familiar, personalized environment that they can access from any number of devices anywhere throughout the enterprise or from home. Administrators gain centralized control, efficiency, and security by having desktop data in the data center.

This chapter includes the following topics:

Advantages of Using VMware Horizon

The benefits of VMware Horizon include simplicity, security, speed, and scale for delivering virtual desktops and applications with cloud-like economics and elasticity.

Flexible VMware Horizon Deployments

VMware Horizon offers the flexibility of deploying virtual desktops and applications on-premises, in a cloud-hosted environment, or a hybrid mix of both. Different deployment environments may require different licenses.

You can deploy VMware Horizon in the following environments.

On-Premises Deployment

VMware Horizon can be deployed on infrastructures on-premises or in a private cloud. You can use a perpetual license for an on-premises deployment. You can optionally purchase the Horizon subscription license which will give you access to the Horizon Control Plane and associated services.

Cloud-Hosted Deployment

VMware Horizon can be deployed in a public cloud, such as VMware Cloud on AWS, or Azure VMware Solutions. You are required to use a subscription license for deployment in a public

cloud. With the subscription license, you will have the options to access the Horizon Control Plane and associated services.

Hybrid Deployment

You can have VMware Horizon deployments on-premises as well as in cloud-hosted environments. You can link these deployments in a federation. In this hybrid deployment scenario, you can have the following deployments:

- Use perpetual license for your on-premise deployments and use subscription license for your cloud-hosted deployments.
- Use subscription license for both your on-premises deployments as well as your cloud-hosted deployments.

Connecting Your Horizon Deployments to Horizon Control Plane

To use the subscription license and access Horizon Control Plane, you must use the Horizon Cloud Connector virtual appliance to connect your Horizon deployment with the Horizon Control Plane.

Horizon Control Plane (enabled by the subscription license) provides the following benefits when connected to your Horizon deployments:

- The Horizon Universal Console provides a single unified console across on-premise and multi-cloud deployments for working with your tenant's fleet of cloud- connected pods.
- Hybrid multi-cloud orchestration provides a single workflow to enable VMware JMP technologies.
- The Horizon Universal Broker is the cloud-based brokering technology used to manage and allocate virtual resources from hybrid multi-cloud assignments to your end users.
- The Cloud Monitoring Service (CMS) is one of the central services provided in Horizon Control Plane. The CMS gives you the ability to monitor capacity, usage, and health within and across your fleet of cloud-connected pods, regardless of the deployment environments in which those individual pods reside.
- The Horizon Image Management Service is a cloud-based service that simplifies and automates the management of system images used by desktop assignments, such as desktop pools and farms, across your cloud-connected Horizon pods.
- The *Horizon Architecture Planning* document provides an overview and requirements of deploying VMware Horizon. For information about Horizon Control Plane, see the VMware Horizon Cloud Service documentation.

Just-in-Time Management Platform (JMP)

JMP represents VMware Horizon capabilities for delivering just-in-time virtual desktops and applications that are flexible, fast, and personalized. JMP includes the following VMware technologies.

Instant Clones

Instant clone is a vSphere-based cloning technology that is used to provision thousands of non-persistent virtual desktops from a single golden image. Instant-clone desktops offer the following advantages:

- Rapid provisioning speed that takes 1-2 seconds on average to create a new desktop.
- Delivers a pristine, high performance desktop every time a user logs in.
- Improves security by destroying the desktop every time a user logs out.
- Eliminates the need to have a dedicated desktop for every single user.
- Zero downtime for patching a pool of desktops.
- You can couple instant clones with VMware App Volumes and VMware Dynamic Environment Manager to deliver fully personalized desktops.

VMware App Volumes

VMware App Volumes is an integrated and unified application delivery and user management system for VMware Horizon and other virtual environments. VMware App Volumes offers the following advantages:

- Quickly provision applications at scale.
- Dynamically attach applications to users, groups, or devices, even when users are already logged in to their desktop.
- Provision, deliver, update, and retire applications in real time.
- Provide a user-writable volume, allowing users to install applications that follow across desktops.

VMware Dynamic Environment Manager

VMware Dynamic Environment Manager offers personalization and dynamic policy configuration across any virtual, physical, and cloud-based environment. VMware Dynamic Environment Manager offers the following advantages:

- Provide end users with quick access to a Windows workspace and applications, with a personalized and consistent experience across devices and locations.
- Simplify end user profile management by providing organizations with a single and scalable solution that leverages the existing infrastructure.
- Speed up the login process by applying configuration and environment settings in an asynchronous process instead of all at login.
- Provide a dynamic environment configuration, such as drive or printer mappings, when a user launches an application.

In addition to utilizing the three underlying JMP technologies, you can also orchestrate their use in a single workflow from the Assignment wizard in the Horizon Control Plane.

Reliability and Security

Desktops and applications can be centralized by integrating with VMware vSphere® and virtualizing server, storage, and networking resources. Placing desktop operating systems and applications on a server in the data center provides the following advantages:

- Access to data can easily be restricted. Sensitive data can be prevented from being copied onto a remote employee's home computer.
- RADIUS support provides flexibility when choosing among two-factor authentication vendors. Supported vendors include RSA SecureID, VASCO DIGIPASS, SMS Passcode, and SafeNet, among others.
- Integration with VMware Workspace ONE Access means that end users have on-demand access to remote desktops through the same web-based application catalog they use to access SaaS, Web, and Windows applications. Inside a remote desktop, users can also use this custom app store to access application. With the True SSO feature, users who authenticate using smart cards or two-factor authentication can access their remote desktops and applications without supplying Active Directory credentials.
- Unified Access Gateway functions as a secure gateway for users who want to access remote desktops and applications from outside the corporate firewall. Unified Access Gateway is an appliance that is installed in a demilitarized zone (DMZ). Use Unified Access Gateway to ensure that the only traffic entering the corporate data center is traffic on behalf of a strongly authenticated remote user.
- The ability to provision remote desktops with pre-created Active Directory accounts addresses the requirements of locked-down Active Directory environments that have read-only access policies.
- Data backups can be scheduled without considering when end users' systems might be turned off.
- Remote desktops and applications that are hosted in a data center experience little or no downtime. Virtual machines can reside on high-availability clusters of VMware servers.
- Virtual desktops can also connect to back-end physical systems and Microsoft Remote Desktop Services (RDS) hosts.

Tight Integration with the VMware Ecosystem

You can use VMware Horizon with VMware vSphere, vSAN, NSX to extend the power of virtualization with virtual compute, virtual storage, and virtual networking and security to drive down costs, enhance the user experience, and deliver greater business agility. You can take your deployment onto a public cloud such as VMware Cloud on AWS or VMware Azure Solutions.

You can also leverage additional management software such as vRealize, Avi Networks, and Carbon Black.

Rich User Experience

VMware Horizon provides the familiar, personalized desktop environment that end users expect, including the following user experiences:

- A rich selection of display protocols.
- Ability to access USB and other devices connected to their local computer.
- Send documents to any printer their local computer can detect.
- Real-time audio/video features.
- Authentication with smart cards.
- Use of multiple display monitors.
- 3D graphics support.

RESTful APIs

VMware Horizon RESTful APIs automate the deployment, operation, management, monitoring, reporting, and analytics for the VMware Horizon infrastructure, workloads, and integration with third-party products. You can use these APIs to perform the following functions:

- Desktop pool management
- Virtual machine and farm management
- Publishing applications
- Entitling published applications
- Infrastructure discovery
- Monitoring and troubleshooting

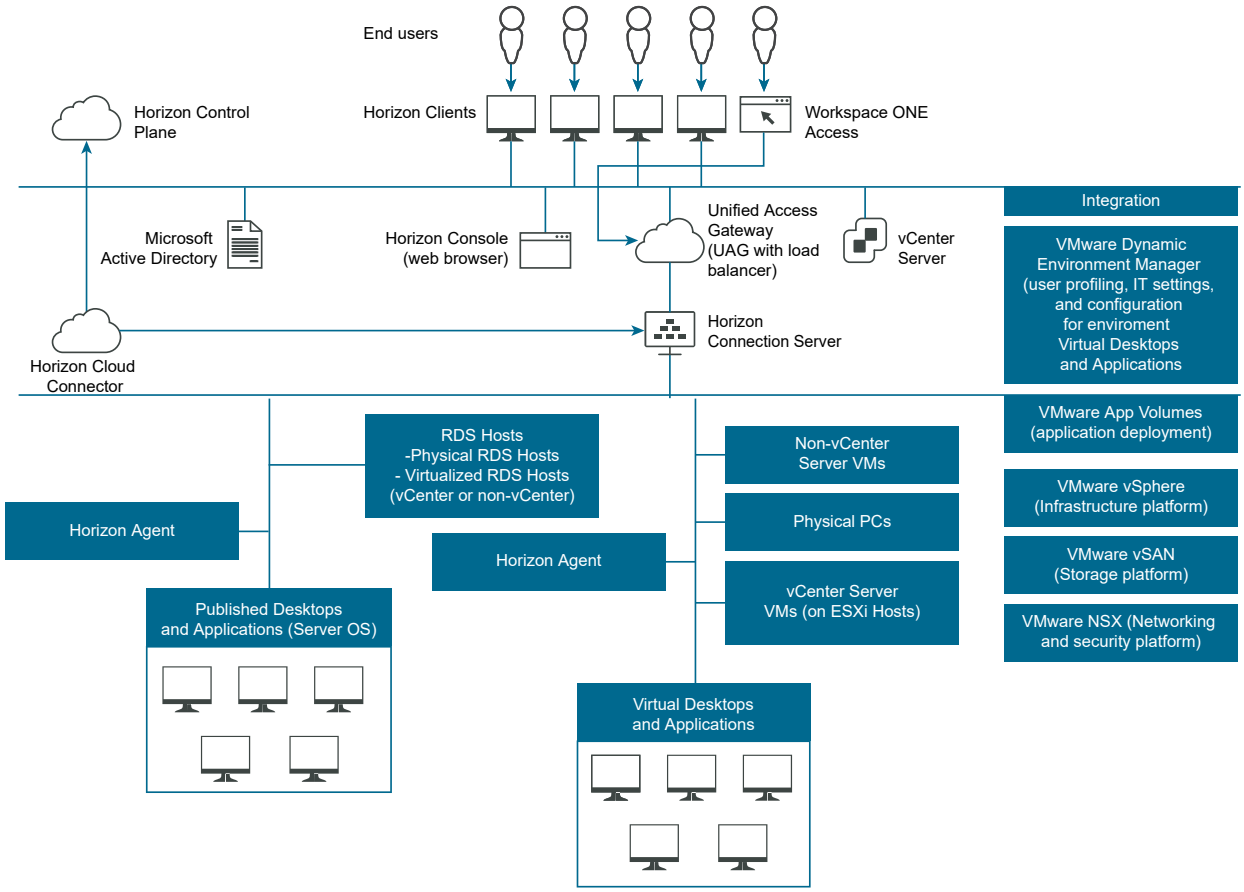
For more information about VMware Horizon REStful APIs, see the RESTful APIs available at https://code.vmware.com/apis/1122/view-rest-api. For a list of Horizon RESTful API for each release, see KB 84155.

How the Components Fit Together

End users start Horizon Client to log in to Horizon Connection Server. This server, which integrates with Windows Active Directory, provides access to remote desktops hosted on a VMware vSphere server, a physical PC, or a Microsoft RDS host. Horizon Client also provides access to published applications on a Microsoft RDS host.

The high-level example of a VMware Horizon environment shows the relationships between the major components of a VMware Horizon deployment.

Figure 1-1. High-Level Example of a VMware Horizon Environment



Client Devices

A major advantage of using VMware Horizon is that remote desktops and applications follow the end user regardless of device or location. Users can access their personalized virtual desktop or remote application from a company laptop, their home PC, a thin client device, a Mac, or a tablet or phone.

End users open Horizon Client to display their remote desktops and applications. Thin client devices use VMware Horizon thin client software and can be configured so that the only application that users can launch directly on the device is VMware Horizon Thin Client. Repurposing a legacy PC into a thin client desktop can extend the life of the hardware by three to five years. For example, by using VMware Horizon on a thin desktop, you can use a newer operating system such as Windows 10 on older desktop hardware.

If you use the HTML Access feature, end users can open a remote desktop inside a browser, without having to install any client application on the client system or device.

Horizon Connection Server

This software service acts as a broker for client connections. Horizon Connection Server authenticates users through Windows Active Directory and directs the request to the appropriate virtual machine, physical PC, or Microsoft RDS host.

Connection Server provides the following management capabilities:

- Authenticating users
- Entitling users to specific desktops and pools
- Managing remote desktop and application sessions
- Establishing secure connections between users and remote desktops and applications
- Enabling single sign-on
- Setting and applying policies

Inside the corporate firewall, you install and configure a group of two or more Connection Server instances. Their configuration data is stored in an embedded LDAP directory and is replicated among members of the group.

Outside the corporate firewall, in the DMZ, you can install install a Unified Access Gateway appliance. Unified Access Gateway appliances in the DMZ communicate with Connection Servers inside the corporate firewall. Unified Access Gateway appliances ensure that the only remote desktop and application traffic that can enter the corporate data center is traffic on behalf of a strongly authenticated user. Users can access only the resources that they are authorized to access.

For more information about Unified Access Gateway appliances, see the Unified Access Gateway documentation at https://docs.vmware.com/en/Unified-Access-Gateway/index.html.

Important It is possible to create a VMware Horizon setup that does not use Connection Server. If you install the View Agent Direct Connect Plugin in a remote virtual machine desktop, the client can connect directly to the virtual machine. All the remote desktop features, including PCoIP, HTML Access, RDP, USB redirection, and session management work in the same way, as if the user had connected through Connection Server. For more information, see the *View Agent Direct-Connection Plugin Administration* document.

Horizon Client

The client software for accessing remote desktops and applications can run on a tablet, a phone, a Windows, Linux, or Mac PC or laptop, a thin client, and more.

After logging in, users select from a list of remote desktops and applications that they are authorized to use. Authorization can require Active Directory credentials, a UPN, a smart card PIN, or an RSA SecurID or other two-factor authentication token.

An administrator can configure Horizon Client to allow end users to select a display protocol. Protocols include PCoIP, Blast Extreme, and Microsoft RDP for remote desktops. The speed and display quality of PCoIP and Blast Extreme rival that of a physical PC.

Features differ according to which Horizon Client you use. This guide focuses on Horizon Client for Windows. The following types of clients are not described in detail in this guide:

- Details about Horizon Client for tablets, Linux clients, and Mac clients. See the Horizon Client documentation at https://docs.vmware.com/en/VMware-Horizon-Client/index.html.
- Details about the HTML Access Web client, which allows you to open a remote desktop inside a browser. No Horizon Client application is installed on the client system or device. See the Horizon Client documentation at https://docs.vmware.com/en/VMware-Horizon-Client/index.html.
- Various third-party thin clients and zero clients, available only through certified partners.

VMware Horizon User Web Portal

From a Web browser on a client device, end users can connect to remote desktops and applications through the browser, automatically start Horizon Client if it is installed, or download the Horizon Client installer.

When you open a browser and enter the URL of a Horizon Connection Server instance, the Web page that appears contains links to the VMware Downloads site for downloading Horizon Client. The links on the Web page are configurable, however. For example, you can configure the links to point to an internal Web server, or you can limit which client versions are available on your own Connection Server.

If you use the HTML Access feature, the Web page also displays a link for accessing remote desktops and applications inside a supported browser. With this feature, no Horizon Client application is installed on the client system or device. For more information, see the Horizon Client documentation at https://docs.vmware.com/en/VMware-Horizon-Client/index.html.

Horizon Agent

You install the Horizon Agent service on all virtual machines, physical systems, and Microsoft RDS hosts that you use as sources for remote desktops and applications. On virtual machines, this agent communicates with Horizon Client to provide features such as connection monitoring, integrated printing, and access to locally connected USB devices.

If the desktop source is a virtual machine, you first install the Horizon Agent service on that virtual machine and then use the virtual machine as a template or as a golden image of instant clones. When you create a pool from this virtual machine, the agent is automatically installed on every remote desktop.

You can install the agent with an option for single sign-on. With single sign-on, users are prompted to log in only when they connect to Horizon Connection Server and are not prompted a second time to connect to a remote desktop or application.

Horizon Console

This web-based application allows administrators to configure Horizon Connection Server, deploy and manage remote desktops and applications, control user authentication, and troubleshoot end user issues.

When you install a Connection Server instance, you also get the URL for the Horizon Console web interface. This web interface allows administrators to manage Connection Server instances from anywhere without having to install an application on their local computer.

vCenter Server

If you are deploying Horizon on vSphere, vCenter Server acts as a central administrator for VMware ESXi servers that are connected on a network. vCenter Server provides the central point for configuring, provisioning, and managing virtual machines in the data center.

In addition to using these virtual machines as sources for virtual machine desktop pools, you can use virtual machines to host the server components of VMware Horizon, including Horizon Connection Server instances, Active Directory servers, Microsoft RDS hosts, and vCenter Server instances.

Integrating VMware Horizon

To enhance the effectiveness of VMware Horizon in your organization, you can use several interfaces to integrate VMware Horizon with external applications or to create administration scripts that you can run from the command line or in batch mode.

Integrating VMware Horizon with Business Intelligence Software

You can configure Horizon Connection Server to record events to a Microsoft SQL Server, Oracle, or PostgreSQL database.

- End-user actions such as logging in and starting a desktop session.
- Administrator actions such as adding entitlements and creating desktop pools.
- Alerts that report system failures and errors.
- Statistical sampling such as recording the maximum number of users over a 24-hour period.

You can use business intelligence reporting engines such as Crystal Reports, IBM Cognos, MicroStrategy 9, and Oracle Enterprise Performance Management System to access and analyze the event database.

For more information, see the *Horizon Administration* document.

You can alternatively generate VMware Horizon events in Syslog format so that the event data can be accessible to analytics software. If you enable file-based logging of events, events are accumulated in a local log file. If you specify a file share, the log files are moved to that share. For more information, see the *Horizon Installation* document.

Using Horizon PowerCLI Cmdlets to Create Administration Scripts

You can use Horizon PowerCLI cmdlets with VMware PowerCLI. Use Horizon PowerCLI cmdlets to perform various administration tasks on Horizon components.

For more information about Horizon PowerCLI cmdlets, read the *VMware PowerCLI Cmdlets Reference* available at https://code.vmware.com/docs/6978/cmdlet-reference.

For information on the API specifications to create advanced functions and scripts to use with Horizon PowerCLI, see the Horizon API Reference at the VMware Developer Center.

For more information on sample scripts that you can use to create your own Horizon PowerCLI scripts, see the Horizon PowerCLI community on GitHub.

You can use the Horizon PowerCLI cmdlets to perform various administration tasks on VMware Horizon components.

- Create and update desktop pools.
- Configure multiple network labels to greatly expand the number of IP addresses assigned to virtual machines in a pool.
- Add data center resources to a full virtual machine.
- Sample the usage of specific desktops or desktop pools over time.
- Query the event database.
- Query the state of services.

Modifying LDAP Configuration Data in VMware Horizon

When you use Horizon Console to modify the configuration of VMware Horizon, the appropriate LDAP data in the repository is updated. Horizon Connection Server stores its configuration information in an LDAP compatible repository. For example, if you add a desktop pool, Connection Server stores information about users, user groups, and entitlements in LDAP.

You can use VMware and Microsoft command-line tools to export and import LDAP configuration data in LDAP Data Interchange Format (LDIF) files from and into VMware Horizon. These commands are for advanced administrators who want to use scripts to update configuration data without using Horizon Console or Horizon PowerCLI.

You can use LDIF files to perform a number of tasks.

- Transfer configuration data between Connection Server instances.
- Define a large number of VMware Horizon objects, such as desktop pools, and add these to your Connection Server instances without using Horizon Console or Horizon PowerCLI.
- Back up a configuration so that you can restore the state of a Connection Server instance.

For more information, see the *Horizon Administration* document.

Using the vdmadmin Command

You can use the `vdmadmin` command line interface to perform a variety of administration tasks on a Connection Server instance. You can use `vdmadmin` to perform administration tasks that are not possible from within the Horizon Console user interface or that need to run automatically from scripts.

For more information, see the *Horizon Administration* document.

Planning a Rich User Experience 2

VMware Horizon provides the familiar, personalized desktop environment that end users expect. For example, on some client systems, end users can access USB and other devices connected to their local computer, send documents to any printer that their local computer can detect, authenticate with smart cards, and use multiple display monitors.

VMware Horizon includes many features that you might want to make available to your end users. Before you decide which features to use, you must understand the limitations and restrictions of each feature.

This chapter includes the following topics:

Feature Support Matrix for Horizon Agent

When planning which display protocol and features to make available to your end users, use the following information to determine which agent (remote desktop and application) operating systems support the feature.

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.

Note For information about which features are supported on the various types of client devices, see the Horizon Client documentation at https://docs.vmware.com/en/VMware-Horizon-Client/index.html.

In addition, several VMware partners offer thin and zero client devices for VMware Horizon deployments. The features that are available for each thin or zero client device are determined by the vendor and model and the configuration that an enterprise chooses to use. For information about the vendors and models for thin and zero client devices, see the VMware Compatibility Guide, available on the VMware Web site.

Choosing a Display Protocol

A display protocol provides end users with a graphical interface to a remote desktop or application that resides in the data center. Depending on which type of client device you have, you can choose from among Blast Extreme and PCoIP (PC-over-IP), which VMware provides, or Microsoft RDP (Remote Desktop Protocol).

You can set policies to control which protocol is used or to allow end users to choose the protocol when they log in to a desktop.

Note For some types of clients, neither the PCoIP nor the RDP remote display protocol is used. For example, if you use the HTML Access client, available with the HTML Access feature, the Blast Extreme protocol is used, rather than PCoIP or RDP. Similarly, if you use a remote Linux desktop, Blast Extreme is used.

VMware Blast Extreme

Optimized for the mobile cloud, VMware Blast Extreme supports the broadest range of client devices that are H.264, HEVC, JPEG, PNG, and proprietary Blast codec capable. Of the display protocols, VMware Blast Extreme offers the lowest CPU consumption for longer battery life on mobile devices. VMware Blast Extreme can compensate for an increase in latency or a reduction in bandwidth and can leverage both TCP and UDP network transports.

The VMware Blast Extreme display protocol can be used for published applications and for remote desktops that use virtual machines or shared-session desktops on an RDS host. The RDS host can be a physical machine or a virtual machine. The VMware Blast display protocol does not operate on a single-user physical computer, except for the enterprise edition of Windows 10 RS4 and later builds.

Note Movies & TV applications are not supported for physical computers running Windows 10 RS4.

VMware Blast Extreme Features

Key features of VMware Blast Extreme include the following:

- Users outside the corporate firewall can use this protocol with the corporate virtual private network (VPN), or users can make secure, encrypted connections to the Unified Access Gateway appliance in the corporate DMZ.

  Note It is not recommened to use VPN since Blast connections are already encrypted. For a better user experience, use the Unified Access Gateway appliance instead.

- Advanced Encryption Standard (AES) 128-bit encryption is supported and is turned on by default. You can, however, change the encryption key cipher to AES-256.
- Connections from all types of client devices.
- Optimization controls for reducing bandwidth usage on the LAN and WAN.
- Performance counters displayed using PerfMon on Windows agents provide an accurate representation of the current state of the system that also updates at a constant rate for the following:
  - Blast session
  - Imaging
  - Audio
  - CDR
  - USB: USB counters displayed using PerfMon on Windows agents are valid if USB traffic is configured to use VMware Virtual Channel (VVC).
  - Skype for Business: counters are for control traffic only.
  - Clipboard
  - RTAV
  - Serial port and scanner redirection features
  - Virtual printing
  - HTML5 MMR
  - Windows Media MMR: Performance counters appear only if you configured this feature to use VMware Virtual Channel (VVC).
- Network continuity during momentary network loss on Windows clients.
- 32-bit color is supported for virtual displays.
- ClearType fonts are supported.
- Audio redirection with dynamic audio quality adjustment for LAN and WAN.
- Real-Time Audio-Video for using webcams and microphones on some client types.

- Copy and paste of text and, on some clients, images between the client operating system and a remote desktop or published application. For other client types, only copy and paste of plain text is supported. You cannot copy and paste system objects such as folders and files between systems.
- Multiple monitors are supported for some client types. On some clients, you can use up to four monitors with a resolution of up to 2560 x 1600 per display or up to three monitors with a resolution of 4K (3840 x 2160) for Windows desktops. Pivot display and autofit are also supported.

  When the 3D feature is enabled, up to two monitors are supported with a resolution of up to 1920 x 1200, or one monitor with a resolution of 4K (3840 x 2160).
- USB redirection is supported for some client types.
- MMR redirection is supported for some Windows client operating systems and some remote desktop operating systems (with Horizon Agent installed).
- Connections to physical machines that have no monitors attached are supported with NVIDIA graphics cards. For best performance, use a graphics card that supports H.264 encoding.

  If you have an add-in discrete GPU and an embedded GPU, the operating system might default to the embedded GPU. To fix this problem, you can disable or remove the device in Device Manager. If the problem persists, you can install the WDDM graphics driver for the embedded GPU, or disable the embedded GPU in the system BIOS. Refer to your system documentation on how disable the embedded GPU.

  Caution Disabling the embedded GPU might cause future loss of access to functionality such as console access to BIOS setup or NT Boot Loader.
- The Blast Codec improves on Adaptive and on H.264 encoders in desktop usage by delivering sharper images and fonts and operates like a video codec with motion detection, motion vectors, and inter-predicted macroblocks. It is supported on the following environments and is disabled by default:
  - Windows and Linux agents. To enable the codec:
    - On a Windows agent, set the registry key: `HKLM\SOFTWARE\VMware, Inc.\VMware Blast\Config\EncoderBlastCodecEnabled = 1`
    - On a Linux agent: `\etc\vmware\config`, set `RemoteDisplay.allowBlastCodec=TRUE`
  - Disable H.264 and HEVC on Windows, Linux, and MacOS client settings. This feature is not supported on mobile clients and the Web client.
- A dynamic encoder switch allows you to switch between a video optimized encoder (H.264 4:2:0 or H.264 4:4:4) and a text optimized encoder (Blast Codec or Adaptive). This switch helps maintain crisp text and video with reduced bandwidth usage. To use this feature, enable the encoder switch:
  - On a Windows agent, set the registry key `HKLM\SOFTWARE\VMware, Inc.\VMware Blast\Config\EncoderSwitchEnabled = 1`

- On a Linux agent: `\etc\vmware\config`, set `RemoteDisplay.allowSwitchEncoder=TRUE`
- Enable Blast Codec, which is disabled by default. If Blast Codec is not enabled, the switch encoder uses Adaptive for text optimized encoding.
- Enable H.264 on Windows, Linux, and MacOS client settings. This feature is not supported on mobile clients and the Web client.

Note The encoder switch only uses software H.264 and does not support hardware-accelerated graphics.

- Blast Extreme implements High Dynamic Range (HDR) encoding, which expands the range of brightness in a digital image to provide a more realistic depiction of a scene. HDR is enabled by default on the agent. You can add these optional registry keys REG_SZ (string value) on a Windows agent:
  - `PixelProviderHDRReferenceWhite`: an integer greater than 0 that controls the relative brightness of the paper white level. The default value is 80.
  - `TopologyHDREnabled = 1` to enable HDR. The default value is 1.
  - `TopologyHDREnabled = 0` to disable HDR.

  On the client, set the optional `HKLM\SOFTWARE\VMware, Inc.\VMware VDM\Client\AllowClientHDR` to True or False for HDR topology requests. The default value is True.

  In the client VMware Blast settings, turn on **Allow High Efficiency Video Decoding (HEVC)** and **Allow High Dynamic Range Decoding (HDR)**.
- You can specify the bandwidth bursting interval for data sent to clients to minimize bandwidth spikes using the registry key MaxBandwidthBurstMsec. The regkey config is a REG_SZ (string value) even though it contains a number. The default is 1000.

  MaxBandwidthBurstMsec configures the interval of time, in milliseconds, during which the network bandwidth can temporarily exceed the bandwidth cap set by MaxBandwidthKbps. For example, if MaxBandwidthKbps = 4000 and MaxBandwidthBurstMsec = 1000, then during a one-second interval the output must not exceed 4 Kbits. However, these 4 Kbits of data can be output as a concentrated burst at the start of the one-second interval or distributed throughout the one-second interval, as needed.

  On a Windows agent, enable the Max Session Bandwidth policy setting, then set the registry key here: `HKLM\SOFTWARE\VMware, Inc.\VMware Blast\Config\MaxBandwidthBurstMsec`
- By default, the VMware Blast session has a maximum bandwidth cap that is proportional to the number of pixels on the remoted screens. You can determine the maximum bandwidth cap, in kilobits per second (Kbps), for a VMware Blast session, based on the total screen area available for the session. This maximum bandwidth cap is calculated from the equation

```
MaxBandwidthCap = Offset + (Slope * ScreenArea)
```

where

- `Offset` is the value, in Kbps, defined by MaxBandwidthKbpsPerMegaPixelOffset. The default is 0.
- `Slope` is the value, in Kbps per megapixel, defined by MaxBandwidthKbpsPerMegaPixelSlope (or corresponding Max Session Bandwidth kbit/s Megapixel Slope GPO). The minimum value is 100. The maximum value is 100000. The default is 6200.
- `ScreenArea` is the total available screen area, in megapixels, of the monitors used to display the Blast session. This megapixel screen area is detected automatically during the session.

Note The maximum bandwidth actually allowed is the **lesser** of the following values:

- The maximum bandwidth configured in the Max Session Bandwidth policy or explicitly via the MaxBandwidthKbps registry key.
- The maximum bandwidth cap calculated from MaxBandwidthKbpsPerMegaPixelOffset and MaxBandwidthKbpsPerMegaPixelSlope (or corresponding Max Session Bandwidth kbit/s Megapixel Slope GPO).

Configurations specified in Group Policies take precedence over configurations made in the corresponding regkey.

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

Wake-on-LAN

Wake-on-LAN is supported for physical machines with the Enterprise edition of Windows 10 RS4 and later. With this feature, users can wake up physical machines when connecting with Horizon Connection Server. The Wake-on-LAN feature has these prerequisites:

- Wake-on-LAN (WoL) is only supported on IPv4 environments.
- The physical machine must be configured to wake up on receiving Wake-on-LAN packets when Wake-on-LAN is enabled in the BIOS settings as well as network card settings.
- Destination port 9 is used for WoL packets from Connection Server.
- WoL packets are IP-directed broadcast packets that must be able to reach Horizon Agent when sent from Horizon Connection Server. Wake-on-LAN functions in these scenarios:
  - Connection Server and Horizon Agent on the physical machine are on the same subnet in a LAN environment.

- All routers between Connection Server and Horizon Agent are configured to allow the IP-directed broadcast packet for the target subnet of the physical machine you want to wake up.

Note The Wake-on-LAN feature does not support floating-assignment pools of a physical Windows 10 agent. The WoL packet is only sent to dedicated assignment pools entitled with a particular user.

Recommended Guest Operating System Settings

1 GB of RAM or more and a dual CPU is recommended for playing in high-definition, full screen mode, or 720p or higher formatted video. To use Virtual Dedicated Graphics Acceleration for graphics-intensive applications such as CAD applications, 4 GB of RAM is required.

Video Quality Requirements

480p-formatted video

You can play video at 480p or lower at native resolutions when the remote desktop has a single virtual CPU. If you want to play the video in high-definition Flash or in full screen mode, the desktop requires a dual virtual CPU. Even with a dual virtual CPU desktop, as low as 360p-formatted video played in full screen mode can lag behind audio, particularly on Windows clients.

720p-formatted video

You can play video at 720p at native resolutions if the remote desktop has a dual virtual CPU. Performance might be affected if you play videos at 720p in high definition or in full screen mode.

1080p-formatted video

If the remote desktop has a dual virtual CPU, you can play 1080p formatted video, although the media player might need to be adjusted to a smaller window size.

3D rendering

You can configure remote desktops to use software- or hardware-accelerated graphics. The software-accelerated graphics feature enables you to run DirectX 9 and OpenGL 2.1 applications without requiring a physical graphics processing unit (GPU). The hardware-accelerated graphics features enable virtual machines to either share the physical GPUs (graphical processing unit) on a vSphere host or dedicate a physical GPU to a single virtual desktop.

For 3D applications, up to two monitors are supported, and the maximum screen resolution is 1920 x 1200.

For more information about 3D features, see Using 3D Graphics Applications.

Hardware Requirements for Client Systems

For information about processor and memory requirements for the specific type of desktop or mobile client device, go to https://docs.vmware.com/en/VMware-Horizon-Client/index.html.

PCoIP

PCoIP (PC over IP) provides an optimized desktop experience for the delivery of a published application or an entire remote desktop environment, including applications, images, audio, and video content for a wide range of users on the LAN or across the WAN. PCoIP can compensate for an increase in latency or a reduction in bandwidth, to ensure that end users can remain productive regardless of network conditions.

The PCoIP display protocol can be used for published applications and for remote desktops that use virtual machines, physical machines that contain Teradici host cards, or shared session desktops on an RDS host.

PCoIP Features

Key features of PCoIP include the following:

- Users outside the corporate firewall can use this protocol with your company's virtual private network (VPN), or users can make secure, encrypted connections to the Unified Access Gateway appliance in the corporate DMZ.
- Advanced Encryption Standard (AES) 128-bit encryption is supported and is turned on by default. You can, however, change the encryption key cipher to AES-256.
- Connections from all types of client devices.
- Optimization controls for reducing bandwidth usage on the LAN and WAN.
- 32-bit color is supported for virtual displays.
- ClearType fonts are supported.
- Audio redirection with dynamic audio quality adjustment for LAN and WAN.
- Real-Time Audio-Video for using webcams and microphones on some client types.
- Copy and paste of text and, on some clients, images between the client operating system and a remote desktop or published application. For other client types, only copy and paste of plain text is supported. You cannot copy and paste system objects such as folders and files between systems.
- Multiple monitors are supported for some client types. On some clients, you can use up to 4 monitors with a resolution of up to 2560 x 1600 per display or up to 3 monitors with a resolution of 4K (3840 x 2160). Pivot display and autofit are also supported.

  When the 3D feature is enabled, up to 2 monitors are supported with a resolution of up to 1920 x 1200, or one monitor with a resolution of 4K (3840 x 2160).
- USB redirection is supported for some client types.

- MMR redirection is supported for some Windows client operating systems and some remote desktop operating systems (with Horizon Agent installed).

For information about which desktop operating systems support specific PCoIP features, see Feature Support Matrix for Horizon Agent.

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

Recommended Guest Operating System Settings

1GB of RAM or more and a dual CPU is recommended for playing in high-definition, full screen mode, or 720p or higher formatted video. To use Virtual Dedicated Graphics Acceleration for graphics-intensive applications such as CAD applications, 4GB of RAM is required.

Video Quality Requirements

480p-formatted video

You can play video at 480p or lower at native resolutions when the remote desktop has a single virtual CPU. If you want to play the video in high-definition Flash or in full screen mode, the desktop requires a dual virtual CPU. Even with a dual virtual CPU desktop, as low as 360p-formatted video played in full screen mode can lag behind audio, particularly on Windows clients.

720p-formatted video

You can play video at 720p at native resolutions if the remote desktop has a dual virtual CPU. Performance might be affected if you play videos at 720p in high definition or in full screen mode.

1080p-formatted video

If the remote desktop has a dual virtual CPU, you can play 1080p formatted video, although the media player might need to be adjusted to a smaller window size.

3D rendering

You can configure remote desktops to use software- or hardware-accelerated graphics. The software-accelerated graphics feature enables you to run DirectX 9 and OpenGL 2.1 applications without requiring a physical graphics processing unit (GPU). The hardware-accelerated graphics features enable virtual machines to either share the physical GPUs (graphical processing unit) on a vSphere host or dedicate a physical GPU to a single virtual machine desktop.

For more information about 3D features, see Using 3D Graphics Applications.

Hardware Requirements for Client Systems

For information about processor and memory requirements, see the "Using VMware Horizon Client" document for the specific type of desktop or mobile client device. Go to https://docs.vmware.com/en/VMware-Horizon-Client/index.html.

Using Published Applications

You can use Horizon Client to securely access published Windows-based applications, in addition to remote desktops.

With this feature, after launching Horizon Client and logging in to a Horizon Connection server, users see all the published applications they are entitled to use, in addition to remote desktops. Selecting an application opens a window for that application on the local client device, and the application looks and behaves as if it were locally installed.

For example, on a Windows client computer, if you minimize the application window, an item for that application remains in the Taskbar and looks identical to the way it would look if it were installed on the local Windows computer. You can also create a shortcut for the application that will appear on your client desktop, just like shortcuts for locally installed applications.

Deploying published applications in this way might be preferable to deploying complete remote desktops under the following conditions:

- If an application is set up with a multi-tiered architecture, where the components work better if they are located geographically near each other, using published applications is a good solution.

  For example, when a user must access a database remotely, if large amounts of data must be transmitted over the WAN, performance is usually affected. With published applications, all parts of the application can be located in the same data center as the database, so that traffic is isolated and only the screen updates are sent across the WAN.
- From a mobile device, accessing an individual application is easier than opening a remote Windows desktop and then navigating to the application.

To use this feature, you install applications on a Microsoft RDS host. In this respect, VMware Horizon published applications work similarly to other application remoting solutions. VMware Horizon published applications are delivered using either the Blast Extreme display protocol or the PCoIP display protocol, for an optimized user experience.

Using USB Devices with Remote Desktops and Applications

Administrators can configure the ability to use USB devices, such as thumb flash drives, cameras, VoIP (voice-over-IP) devices, and printers, from a virtual desktop. This feature is called USB redirection. A virtual desktop can accommodate up to 255 USB devices.

You can also redirect certain locally connected USB devices for use in published desktops and applications. For information about the specific types of devices that are supported, see the *Configuring Remote Desktop Features in Horizon* document.

When you use this feature in desktop pools that are deployed on single-user machines, most USB devices that are attached to the local client system become available in the remote desktop. You can even connect to and manage an iPad from a remote desktop. For example, you can sync your iPad with iTunes installed in your remote desktop. On some client devices, such as Windows and Mac computers, the USB devices are listed in a menu in Horizon Client. You use the menu to connect and disconnect the devices.

In most cases, you cannot use a USB device in your client system and in your remote desktop at the same time. Only a few types of USB devices can be shared between a remote desktop and the local computer. These devices include smart card readers and human interface devices, such as keyboards and pointing devices.

Administrators can specify the types of USB devices to which end users are allowed to connect. For composite devices that contain multiple types of devices, such as a video input device and a storage device, on some client systems, administrators can split the device so that one device (for example, the video input device) is allowed but the other device (for example, the storage device) is not.

The USB redirection feature is available only on certain types of clients. To find out whether this feature is supported on a particular client, see the feature support matrix included in the Horizon Client installation and setup document for that client.

Using Webcams and Microphones

With the Real-Time Audio-Video feature, you can use the local client system's webcam or microphone in a remote desktop or published application. Real-Time Audio-Video is compatible with standard conferencing applications and browser-based video applications. It supports standard webcams, audio USB devices, and analog audio input.

End users can run Skype, Webex, Google Hangouts, and other online conferencing applications in their remote desktops. This feature redirects video and audio data to the agent machine with a lower bandwidth than can be achieved by using USB redirection. With Real-Time Audio-Video, webcam images and audio input are encoded on the client system and then sent to the agent machine. On the agent machine, a virtual webcam and virtual microphone can decode and play the stream, which the third-party application can use.

No special configuration is necessary, although administrators can set agent-side group policies and registry keys to configure frame rate and image resolution, or to turn off the feature. By default, the resolution is 320 by 240 pixels at 15 frames per second. If needed, administrators can also use client-side configuration settings to set a preferred webcam or audio device.

Note This feature is available only on some types of clients. To find out whether this feature is supported on a particular type of client, see the feature support matrix included in the installation and setup document for the specific type of desktop or mobile client device.

Using 3D Graphics Applications

The software- and hardware-accelerated graphics features available with the Blast Extreme or PCoIP display protocol enable remote desktop users to run 3D applications ranging from Google Earth to CAD and other graphics-intensive applications.

NVIDIA GRID vGPU (shared GPU hardware acceleration)

Available with vSphere, this feature allows a physical GPU (graphical processing unit) on an ESXi host to be shared among virtual machines. Use this feature if you require high-end, hardware-accelerated workstation graphics.

AMD MxGPU

Available with vSphere, this feature allows multiple virtual machines to share an AMD GPU by making the GPU appear as multiple PCI passthrough devices. This feature offers flexible hardware-accelerated 3D profiles, ranging from lightweight 3D task workers to high-end workstation graphics power users.

Virtual Dedicated Graphics Acceleration (vDGA)

Available with vSphere, this feature dedicates a single physical GPU on an ESXi host to a single virtual machine. Use this feature if you require high-end, hardware-accelerated workstation graphics.

Note See the VMware Hardware Compatibility List at http://www.vmware.com/resources/compatibility/search.php. For Intel vDGA, the Intel integrated GPU is used rather than discrete GPUs, as is the case with other vendors.

Virtual Shared Graphics Acceleration (vSGA)

Available with vSphere, this feature allows multiple virtual machines to share the physical GPUs on ESXi hosts. You can use 3D applications for design, modeling, and multimedia.

Soft 3D

Software-accelerated graphics, available with vSphere, allows you to run DirectX 9 and OpenGL 2.1 applications without requiring a physical GPU. Use this feature for less demanding 3D applications such as Windows Aero themes, Microsoft Office 2010, and Google Earth.

Important See the VMware resource Deploying Hardware-Accelerated Graphics with VMware Horizon. The rendering options differ by environment (vSphere, non-vSphere, and physical PC) and use cases (virtual desktops versus published desktops). See the *Setting Up Published Desktops and Applications in Horizon* document for the 3D options available specific to your environment and use case. For more information on the various choices for 3D rendering, see the NVIDIA GRID vGPU Deployment Guide for VMware Horizon 6.1, and NVIDIA GRID Virtual GPU User Guide.

Streaming Multimedia to a Remote Desktop

The Windows Media MMR (multimedia redirection) feature, for desktops and clients, enables full-fidelity playback on client computers when multimedia files are streamed to a remote desktop.

With MMR, the multimedia stream is processed, that is, decoded, on the client system. The client system plays the media content, thereby offloading the demand on the ESXi host. Media formats that are supported on Windows Media Player are supported; for example: M4V; MOV; MP4; WMP; MPEG-4 Part 2; WMV 7, 8, and 9; WMA; AVI; ACE; MP3; WAV.

Note You must add the MMR port as an exception to your firewall software. The default port for MMR is 9427 for a PCoIP connection.

Printing from a Remote Desktop

The virtual printing feature allows end users on some client systems to use local or network printers from a remote desktop without requiring that additional print drivers be installed in the remote desktop operating system. The location-based printing feature allows you to map remote desktops to the printer that is closest to the endpoint client device.

With virtual printing, after a printer is added on a local client computer, that printer is automatically added to the list of available printers on the remote desktop. No further configuration is required. For each printer available through this feature, you can set preferences for data compression, print quality, double-sided printing, color, and so on. Users who have administrator privileges can still install printer drivers on the remote desktop without creating a conflict with the virtual printing component.

Local printer redirection is designed for the following use cases:

- Printers directly connected to USB or serial ports on the client device
- Specialized printers such as bar code printers and label printers connected to the client
- Network printers on a remote network that are not addressable from the virtual session.

To send print jobs to a USB printer, you can either use the USB redirection feature or use the virtual printing feature.

Location-based printing allows IT organizations to map remote desktops to the printer that is closest to the endpoint client device. For example, as a doctor moves from room to room in a hospital, each time the doctor prints a document, the print job is sent to the nearest printer. Using this feature does require that the correct printer drivers be installed in the remote desktop.

Note These printing features are available only on some types of clients. To find out whether a printing feature is supported on a particular type of client, see the feature support matrix included in the installation and setup guide for the specific type of desktop or mobile client device. Go to https://docs.vmware.com/en/VMware-Horizon-Client/index.html.

Using Single Sign-On for Logging In

The single-sign-on (SSO) feature allows end users to supply Active Directory login credentials only once.

If you do not use the single-sign-on feature, end users must log in twice. They are first prompted for Active Directory credentials to log in to Horizon Connection Server and then are prompted log in to their remote desktop. If smart cards are also used, end users must sign in three times because users must also log in when the smart card reader prompts them for a PIN.

For remote desktops, this feature includes a credential provider dynamic-link library.

True SSO

With the True SSO feature, users are no longer required to supply Active Directory credentials at all. After users log in to VMware Identity Manager using any non-AD method (for example, RSA SecurID or RADIUS authentication), users are not prompted to also enter Active Directory credentials in order to use a remote desktop or application.

If a user authenticates by using smart cards or Active Directory credentials, the True SSO feature is not necessary, but you can configure True SSO to be used even in this case. Then any AD credentials that the user provides are ignored and True SSO is used.

True SSO works by generating a unique, short-lived certificate for the Windows logon process. You must set up a Certificate Authority, if you do not already have one, and a certificate Enrollment Server in order to generate short-lived certificates on behalf of the user. You install the Enrollment Server by running the Connection Server installer and selecting the Enrollment Server option.

True SSO separates authentication (validating a user's identity) from access (such as to a Windows desktop or application). User credentials are secured by a digital certificate. No passwords are vaulted or transferred within the data center. For more information, see the *Horizon Administration* document.

Monitors and Screen Resolution

You can extend a remote desktop to multiple monitors. If you have a high-resolution monitor, you can see the remote desktop or application in full resolution.

You can select the All Monitors display mode to display a remote desktop on multiple monitors. If you are using All Monitors mode and click the Minimize button, if you then maximize the window, the window goes back to All Monitors mode. Similarly, if you are using Fullscreen mode and minimize the window, when you maximize the window, the window goes back to Fullscreen mode on one monitor.

Using All Monitors in a Multiple-Monitor Setup

Regardless of the display protocol, you can use multiple monitors with a remote desktop. If you have Horizon Client use all monitors, if you maximize an application window, the window expands to the full screen of only the monitor that contains it.

Horizon Client supports the following monitor configurations:

- If you use two monitors, the monitors are not required to be in the same mode. For example, if you are using a laptop connected to an external monitor, the external monitor can be in portrait mode or landscape mode.
- Monitors can be placed side by side, stacked two by two, or vertically stacked only if you are using two monitors and the total height is less than 4096 pixels.
- To use the 3D rendering feature, you must use the VMware Blast display protocol or the PCoIP display protocol. You can use up to two monitors, with a resolution of up to 1920 x 1200. For a resolution of 4K (3840 x 2160), only one monitor is supported.
- - Windows Server 2019 virtual desktops require Horizon Agent 7.7 or later.
  - Windows 7 and Windows 8.x virtual desktops are not supported with Horizon Agent 2006 and later.
- With the VMware Blast display protocol, a remote desktop screen resolution of 8K (7680 x 4320) is supported. Two 8K displays are supported. The hardware version of the desktop virtual machine must be 14 (ESXi 6.7 or later). You must allocate sufficient system resources in the virtual machine to support an 8K display. For information about supported monitor configurations for GRID-based desktops, and for NVIDIA vGPU profiles, see the *Virtual GPU Software User Guide* on the NVIDIA website. This feature is supported only with the Windows client.
- With the VMware Blast display protocol or the PCoIP display protocol, a remote desktop screen resolution of 4K (3840 x 2160) is supported. The number of 4K displays that are supported depends on the hardware version of the desktop virtual machine and the Windows 10 version.

Hardware Version	Number of 4K Displays Supported
10 (ESXi 5.5.x compatible)	1
11 (ESXi 6.0 compatible)	3
11	1
13, 14, or later	1 (3D rendering feature enabled) 4 (3D rendering feature disabled)

For the best performance, the virtual machine should have at least 2 GB of RAM and 2 vCPUs. This feature might require good network conditions, such as a bandwidth of 1000 Mbps with low network latency and a low package loss rate.

Note When the remote desktop screen resolution is set to 3840 x 2160 (4K), items on the screen might appear smaller, and you might not be able to use the Screen Resolution dialog box in the remote desktop to make text and other items larger. On a Windows client, you can set the client machine's DPI to the proper setting and enable the DPI Synchronization feature to redirect the client machine's DPI setting to the remote desktop.

- If you use Microsoft RDP 7, the maximum number of monitors that you can use to display a remote desktop is 16.
- If you use Microsoft RDP display protocol, you must have Microsoft Remote Desktop Connection (RDC) 6.0 or later installed in the remote desktop.

Using One Monitor in a Multiple-Monitor Setup

If you have multiple monitors but want Horizon Client to use only one monitor, you can select to have a remote desktop window open in any mode other than All Monitors. By default, the window is opened on the primary monitor. For more information, see the *VMware Horizon Client for Windows Installation and Setup Guide* document.

Using High-Resolution Mode

On some types of clients, when you use the VMware Blast display protocol or the PCoIP display protocol, Horizon Client also supports very high resolutions for those client systems with high-resolution displays. The option to enable High-Resolution Mode appears only if the client system supports high-resolution displays.

Hardware encoding is enabled by default after you have vGPU configured in the virtual machine. Hardware encoding is enabled for all supported multiple-monitor configurations, except vGPU profiles that use less than 1 GB of video memory will use the software decoder due to NVENC memory restrictions. See *NVENC requires at least 1 Gbyte of frame buffer* in https://docs.nvidia.com/grid/4.3/grid-vgpu-release-notes-vmware-vsphere/index.html

Managing Desktop and Application Pools from a Central Location

3

You can create pools that include one or thousands of remote desktops. As a desktop source, you can use virtual machines, physical machines, and Windows Remote Desktop Services (RDS) hosts. Create one virtual machine as a base image, and VMware Horizon can generate a pool of remote desktops from that image. You can also create pools of applications that give users remote access to applications.

This chapter includes the following topics:

Desktop Pools

VMware Horizon offers the ability to create and provision pools of desktops as its basis of centralized management.

You create a desktop pool from one of the following sources:

- A virtual machine that is hosted on an ESXi host and managed by vCenter Server.
- A session-based desktop on an RDS host. For more information about creating desktop pools from an RDS host, see the *Setting Up Published Desktops and Applications in Horizon* in Horizon document.
- A non-vSphere machine such as a physical desktop PC.
- A virtual machine that runs on a virtualization platform other than vCenter Server that supports Horizon Agent.

If you use a vSphere virtual machine as a desktop source, you can automate the process of making as many identical virtual desktops as you need. You can set a minimum and maximum number of virtual desktops to be generated for the pool. Setting these parameters ensures that you always have enough remote desktops available for immediate use but not so many that you overuse available resources.

Using pools to manage desktops allows you to apply settings or deploy applications to all remote desktops in a pool. For more information about desktop pools of virtual machines or unmanaged machines, see the *Setting Up Virtual Desktops in Horizon* document. For more information about desktop pools based on sessions on RDS hosts, see the *Setting Up Published Desktops and Applications in Horizon* document.

Application Pools

With application pools that run on a farm of RDS hosts, you give users access to published applications that run on servers in a data center instead of on their personal computers or devices.

Application pools offer several important benefits:

- Accessibility

  Users can access applications from anywhere on the network. You can also configure secure network access.

- Device independence

  With application pools, you can support a range of client devices, such as smart phones, tablets, laptops, thin clients, and personal computers. The client devices can run various operating systems, such as Windows, iOS, Mac OS, or Android.

- Access control

  You can easily and quickly grant or remove access to applications for one user or a group of users.

- Accelerated deployment

  With application pools, deploying applications can be accelerated because you only deploy applications on servers in a data center and each server can support multiple users.

- Manageability

  Managing software that is deployed on client computers and devices typically requires significant resources. Management tasks include deployment, configuration, maintenance, support, and upgrades. With application pools, you can simplify software management in an enterprise because the software runs on servers in a data center, which requires fewer installed copies.

- Security and regulatory compliance

  With application pools, you can improve security because applications and their associated data are centrally located in a data center. Centralized data can address security concerns and regulatory compliance issues.

- Reduced cost

  Depending on software license agreements, hosting applications in a data center can be more cost-effective. Other factors, including accelerated deployment and improved manageability, can also reduce the cost of software in an enterprise.

Application Provisioning

With VMware Horizon, you have several options regarding application provisioning.

- Deploy published applications using RDS hosts. See Deploying Published Applications Using an RDS Host.s
- Deploy published applications that run on desktop pools with VM Hosted Applications. See Deploying Published Applications That Run On Desktop Pools With VM Hosted Applications.
- Deploy applications within virtual desktops. See Deploying Applications Within Virtual Desktops.
- Deploy applications using VMware App Volumes. You can package applications and deliver them to your users using VMware App Volumes. As your users log into their remote desktops, their apps will be attached to their desktops, Fore more information, see the VMware App Volumes documentation at https://docs.vmware.com/en/VMware-App-Volumes/index.html.
- Distribute application packages created with VMware ThinApp. For more information about distributing application packages created with VMware ThinApp, see the VMware ThinApp documentation at https://docs.vmware.com/en/VMware-ThinApp/index.html.
- Deploying Published Applications Using an RDS Host

  You might choose to provide end users with published applications rather than remote desktops. Individual published applications might be easier to navigate on a small mobile device.
- Deploying Published Applications That Run On Desktop Pools With VM Hosted Applications

  You can deliver one or multiple published applications to end users without creating a farm of RDS hosts. You can create a pool of virtual machine desktops to host the applications and then expose end users to only the published applications.
- Deploying Applications Within Virtual Desktops

  You can deploy applications into the golden image, and create a pool of identical desktops each with the exact same copy of applications.

Deploying Published Applications Using an RDS Host

You might choose to provide end users with published applications rather than remote desktops. Individual published applications might be easier to navigate on a small mobile device.

End users can access published Windows-based applications by using the same Horizon Client that they previously used for accessing remote desktops, and they use the same Blast Extreme or PCoIP display protocol.

To provide a published application, you install the application on a Microsoft Remote Desktop Session (RDS) host. One or more RDS hosts make up a farm, and from that farm administrators create application pools in a similar manner to creating desktop pools. For farm sizing recommendations see the VMware Knowledge Base (KB) article http://kb.vmware.com/kb/2150348.

Using this strategy simplifies adding, removing, and updating applications; adding or removing user entitlements to applications; and providing access from any device or network to centrally or distributed application farms.

Deploying Published Applications That Run On Desktop Pools With VM Hosted Applications

You can deliver one or multiple published applications to end users without creating a farm of RDS hosts. You can create a pool of virtual machine desktops to host the applications and then expose end users to only the published applications.

This approach benefits the following applications types.

This strategy simplifies the use of the following application types.

- Applications that require .NET framework version compatibility.
- Applications that require special device support, where drivers may not run or be supported on RDS Hosts.
- Applications that are only tested and certified on Windows 10.
- Applications that require an install license and usage reporting by independent software vendors.

For more information, see the "Best Practices for Published Applications and Desktops in VMware Horizon and VMware Horizon Apps" document available at https://techzone.vmware.com.

Deploying Applications Within Virtual Desktops

You can deploy applications into the golden image, and create a pool of identical desktops each with the exact same copy of applications.

If you are deploying an instant-clone desktop pool, when the time comes to patch the applications across all the desktops, you can simply update the golden image and use the push image feature to quickly propagate the changes across all the desktops in the pool on a rolling basis. When a user logs off an instant-clone virtual desktop, VMware Horizon deletes the instant clone and creates a fresh new instant clone from the latest version of the golden image. This new clone is ready for the next user to log in. With rolling updates, the downtime associated with pool maintenance can be minimized.

You can use this feature for the following tasks:

- Applying operating system and software patches and upgrades
- Applying service packs
- Adding applications
- Adding virtual devices
- Changing other virtual machine settings, such as available memory

Using Active Directory GPOs to Manage Users and Desktops

VMware Horizon includes many Group Policy administrative ADMX templates for centralizing the management and configuration of VMware Horizon components and remote desktops.

After you import these templates into Active Directory, you can use them to set policies that apply to the following groups and components:

- All systems regardless of which user logs in
- All users regardless of the system they log in to
- Connection Server configuration
- Horizon Client configuration
- Horizon Agent configuration

After a GPO is applied, properties are stored in the local Windows registry of the specified component.

You can use GPOs to set all the policies that are available from the Horizon Console web interface. You can also use GPOs to set policies that are not available from the UI. For a complete list and description of the settings available through ADMX templates, see the *Configuring Remote Desktop Features in Horizon* document.

Using Smart Policies with Dynamic Environment Manager

You can also use Smart Policies to create policies that control the behavior of the USB redirection, virtual printing, clipboard redirection, client drive redirection, and PCoIP display protocol features on specific remote desktops. This feature requires Dynamic Environment Manager.

With Smart Policies, you can create policies that take effect only if certain conditions are met. For example, you can configure a policy that disables the client drive redirection feature if a user connects to a remote desktop from outside your corporate network.

In general, Horizon policy settings that you configure for remote desktop features in Dynamic Environment Manager override any equivalent registry key and group policy settings.

Architecture Design Elements and Planning Guidelines for Remote Desktop Deployments

4

This chapter discusses architecture design elements and planning guidelines that includes key details about requirements for memory, CPU, storage capacity, network components, and hardware to give IT architects and planners a practical understanding of what is involved in deploying a VMware Horizon solution.

For details on how to architect a VMware Horizon deployment, see the "VMware Workspace ONE and VMware Horizon Reference Architecture" document available at https://techzone.vmware.com.

Important This chapter does not cover the following topics:

Architecture design for hosted applications	A VMware Horizon pod can support farms of Microsoft RDS hosts, where each farm contains RDS hosts. For more information, see the *Setting Up Published Desktops and Applications in Horizon* document. If you plan to use virtual machines for RDS hosts, also see RDS Host Virtual Machine Configuration.
Architecture design for View Agent Direct-Connection Plugin	With this plugin running on a remote virtual machine desktop, the client can connect directly to the virtual machine. All the remote desktop features, including PCoIP, HTML Access, RDP, USB redirection, and session management work in the same way, as if the user had connected through View Connection Server. For more information, see the *View Agent Direct-Connection Plugin Administration* document.

This chapter includes the following topics:

Guest Operating System Requirements for Remote Desktops

When you plan the specifications for remote desktops, the choices that you make regarding RAM, CPU, and disk space have a significant effect on your choices for server and storage hardware and expenditures.

- Planning Based on Types of Workers

  For many configuration elements, including RAM, CPU, and storage sizing, requirements depend largely on the type of worker who uses the virtual desktop and on the applications that must be installed.

- Desktop Types

  The most fundamental question to consider is whether a certain type of user needs a stateful desktop image or a stateless desktop image. Whether you use persistent or non-persistent desktops depends on the specific type of worker.

- Estimating Memory Requirements for Virtual Machine Desktops

  RAM costs more for servers than it does for PCs. Because the cost of RAM is a high percentage of overall server hardware costs and total storage capacity needed, determining the correct memory allocation is crucial to planning your desktop deployment.

- Estimating CPU Requirements for Virtual Machine Desktops

  When estimating CPU, you must gather information about the average CPU utilization for various types of workers in your enterprise.

- Choosing the Appropriate System Disk Size

  When allocating disk space, provide only enough space for the operating system, applications, and additional content that users might install or generate. Usually this amount is smaller than the size of the disk that is included on a physical PC.

- Desktop Virtual Machine Configuration

  The example settings for items such as memory, number of virtual processors, and disk space are specific to VMware Horizon.

- RDS Host Virtual Machine Configuration

  Use RDS (Remote Desktop Services) hosts for providing published applications and session-based remote desktops to end users.

Planning Based on Types of Workers

For many configuration elements, including RAM, CPU, and storage sizing, requirements depend largely on the type of worker who uses the virtual desktop and on the applications that must be installed.

For architecture planning, workers can be categorized into several types.

Task workers

Task workers and administrative workers perform repetitive tasks within a small set of applications, usually at a stationary computer. The applications are usually not as CPU- and memory-intensive as the applications used by knowledge workers. Task workers who work specific shifts might all log in to their virtual desktops at the same time. Task workers include call center analysts, retail employees, warehouse workers, and so on.

Knowledge workers

Knowledge workers' daily tasks include accessing the Internet, using email, and creating complex documents, presentations, and spreadsheets. Knowledge workers include accountants, sales managers, marketing research analysts, and so on.

Power users

Power users include application developers and people who use graphics-intensive applications. These users and applications tend to be CPU and memory intensive and therefore these considerations should be made in the architecture process.

Kiosk users

These users need to share a desktop that is located in a public place. Examples of kiosk users include students using a shared computer in a classroom, nurses at nursing stations, and computers used for job placement and recruiting. These desktops require automatic login. Authentication can be done through certain applications if necessary.

Desktop Types

The most fundamental question to consider is whether a certain type of user needs a stateful desktop image or a stateless desktop image. Whether you use persistent or non-persistent desktops depends on the specific type of worker.

Persistent Desktop

Persistent desktops have data in the operating system image itself that must be preserved, maintained, and backed up. For example, users who need to install some of their own applications or have data that cannot be saved outside of the virtual machine itself (such as on a file server or in an application database) require a persistent desktop.

There are several ways to create persistent desktops in VMware Horizon:

You can create automated pools of full-clone virtual machines.

If you already have virtual desktops or physical desktops created (vCenter virtual machines, non-vCenter virtual machines, or physical PCs), you can import them into VMware Horizon as persistent desktops using the manual desktop pool with a dedicated-assignment.

Persistent desktops give users the highest degree of flexibility and control over their own desktops. However, they consume more compute resources and are more difficult to manage by IT. These desktops might require traditional image management techniques. Persistent desktops can have low storage costs in conjunction with certain storage system technologies. Since each persistent desktop is unique and must be preserved, backup and recovery technologies are important when considering strategies for business continuity.

Non-persistent Desktop

Non-persistent desktops are stateless images that are identical to one another. They are primarily used by users who do not need to install or preserve their own applications. Non-persistent desktops have many advantages, such as being easier to support and having lower storage costs. Other benefits include a limited need to back up the virtual machines and easier, less expensive disaster recovery and business continuity options. The virtual desktops themselves do not need to be protected as there is no unique user data stored. In the event that the virtual desktops are destroyed, you can simply re-create them from the golden image. Folder redirection and various profile technologies can optionally be used to storage user profile and user data.

In VMware Horizon, you can create non-persistent desktops by leveraging instant clones. For more information on instant clones, see the *Setting Up Virtual Desktops in Horizon* document.

Desktops for Task Workers

Since task workers perform repetitive tasks within a small set of applications, you can utilize non-persistent desktops, which saves on storage an compute costs and make desktop management easier.

Desktops for Knowledge Workers and Power Users

Knowledge workers are usually required to create complex documents and have them persist. Power users often need to install their own applications and have them persist. Depending on the nature and amount of personal data that must be retained, they require either a non-persistent desktop or a persistent desktop.

For workers who must install their own applications, which adds data to the operating system disk, the best option is to create a persistent desktop using full clone virtual machines.

Desktops for Kiosk Users

Kiosk users might include customers at airline check-in stations, students in classrooms or libraries, medical personnel at medical data entry workstations, or customers at self-service points. Accounts associated with client devices rather than users are entitled to use these desktop pools because users do not need to log in to use the client device or the remote desktop. Users can still be required to provide authentication credentials for some applications.

Virtual machine desktops that are set to run in kiosk mode use non-persistent desktops because user data does not need to be preserved in the operating system disk. Kiosk mode desktops are used with thin client devices or locked-down PCs. You must ensure that the desktop application implements authentication mechanisms for secure transactions, that the physical network is secure against tampering and snooping, and that all devices connected to the network are trusted.

To set up kiosk mode, you must use the `vdmadmin` command-line interface and perform several procedures documented in the topics about kiosk mode in the *Horizon Administration* document.

For more information creating desktop pools for specific types of workers, see the *Setting Up Virtual Desktops in Horizon* document.

Estimating Memory Requirements for Virtual Machine Desktops

RAM costs more for servers than it does for PCs. Because the cost of RAM is a high percentage of overall server hardware costs and total storage capacity needed, determining the correct memory allocation is crucial to planning your desktop deployment.

If the RAM allocation is too low, it can affect storage I/O because too much Windows paging occurs. If the RAM allocation is too high, it can affect storage capacity because the paging file in the guest operating system and the swap and suspend files for each virtual machine become too large.

RAM Sizing Impact on Performance

When allocating RAM, avoid selecting an overly conservative setting. Consider the following:

- Insufficient RAM allocations can cause excessive Windows paging, which can generate I/O that causes significant performance degradations and increases storage I/O load.
- Because virtual desktop performance is sensitive to response times, VMware recommends reserving all the memory.

RAM Sizing Impact on Storage

The amount of RAM that you allocate to a virtual machine is directly related to the size of the certain files that the virtual machine uses. To access the files in the following list, use the Windows guest operating system to locate the Windows page and hibernate files, and use the ESXi host's file system to locate the ESXi swap and suspend files.

Windows page file

By default, this file is sized at 150 percent of guest RAM. This file, which is by default located at `C:\pagefile.sys`, causes thin-provisioned storage to grow because it is accessed frequently.

For instant clones, any guest operating systems paging and temp files are automatically deleted during the logoff operation and so do not have time to grow very large. Each time a user logs out of an instant clone desktop, Horizon deletes the clone, and provisions and powers on another instant clone based on the latest OS image available for the pool.

Windows hibernate file for laptops

This file can equal 100 percent of guest RAM. You can safely delete this file because it is not needed in Horizon deployments.

ESXi swap file

This file, which has a `.vswp` extension, is created if you reserve less than 100 percent of a virtual machine's RAM. The size of the swap file is equal to the unreserved portion of guest RAM. For example, if 50 percent of guest RAM is reserved and guest RAM is 2 GB, the ESXi swap file is 1 GB. This file can be stored on the local data store on the ESXi host or cluster.

ESXi suspend file

This file, which has a `.vmss` extension, is created if you set the desktop pool logoff policy so that the virtual desktop is suspended when the end user logs off. The size of this file is equal to the size of guest RAM.

RAM Sizing for Specific Monitor Configurations When Using PCoIP or Blast Extreme

In addition to system memory, a virtual machine also requires a small amount of RAM on the ESXi host for video overhead. This VRAM size requirement depends in on the display resolution and number of monitors configured for end users. Table 4-1. PCoIP or Blast Extreme Client Display Overhead lists the amount of overhead RAM required for various configurations. The amounts of memory listed in the columns are in addition to the amount of memory required for other PCoIP or Blast Extreme functionality.

Note 5K and 8K UHD resolutions are only available when using the Blast protocol and only for 1-monitor or 2-monitor configurations. If you attempt to launch a PCoIP session with a 5K or 8K monitor configured on the client, the session fails.

Table 4-1. PCoIP or Blast Extreme Client Display Overhead

Display Resolution Standard	Width (Pixels)	Height (Pixels)	1-Monitor Overhead (MB)	2-Monitor Overhead (MB)	3-Monitor Overhead (MB)	4-Monitor Overhead (MB)
VGA	640	480	1.20	3.20	4.80	5.60
WXGA	1280	800	4.00	12.50	18.75	25.00
1080p	1920	1080	8.00	25.40	38.00	50.60
WQXGA	2560	1600	16.00	60.00	84.80	109.60
UHD (4K)	3840	2160	32.00	78.00	124.00	170.00

Table 4-1. PCoIP or Blast Extreme Client Display Overhead (continued)

Display Resolution Standard	Width (Pixels)	Height (Pixels)	1-Monitor Overhead (MB)	2-Monitor Overhead (MB)	3-Monitor Overhead (MB)	4-Monitor Overhead (MB)
5K Blast only	5120	2880	64.00	128.00	NA	NA
UHD (8K) Blast only	7680	4320	128.00	256.00	NA	NA

For calculating system requirements, the VRAM values are in addition to the base system RAM for the virtual machine. The system automatically calculates and configures overhead memory when you specify the maximum number of monitors and select the display resolution in Horizon Console.

If you use the 3D rendering feature and select Soft3D or vSGA, you can recalculate using the additional VRAM values in a Horizon Console control for configuring VRAM for 3D guests. Alternatively, and for other types of graphics acceleration besides Soft3D and vSGA, you can specify the exact amount of VRAM if you elect to manage VRAM by using vSphere Client.

By default, the multiple-monitor configuration matches the host topology. There is extra overhead pre-calculated for more than two monitors to accommodate additional topology schemes. If you encounter a black screen when starting a remote desktop session, verify that the values for the number of monitors and the display resolution, which are set in Horizon Console, match the host system, or manually adjust the amount of memory by using selecting **Manage using vSphere Client** in Horizon Console and then set the total video memory value to maximum of 128MB.

RAM Sizing for Specific Workloads and Operating Systems

Because the amount of RAM required can vary widely, depending on the type of worker, many companies conduct a pilot phase to determine the correct setting for various pools of workers in their enterprise.

A good starting point is to allocate 2 GB for Windows 10 or later desktops. If you want to use one of the hardware accelerated graphics features for 3D workloads, VMware recommends two virtual CPUs and 4 GB of RAM. During a pilot, monitor the performance and disk space used with various types of workers and make adjustments until you find the optimal setting for each pool of workers.

Estimating CPU Requirements for Virtual Machine Desktops

When estimating CPU, you must gather information about the average CPU utilization for various types of workers in your enterprise.

CPU requirements vary by worker type. During your pilot phase, use a performance monitoring tool, such as Perfmon in the virtual machine, `esxtop` in ESXi, or vCenter Server performance monitoring tools, to understand both the average and peak CPU use levels for these groups of workers. Also use the following guidelines:

- Software developers or other power uses with high-performance needs might have much higher CPU requirements than knowledge workers and task workers. Dual or Quad virtual CPUs are recommended for 64-bit Windows virtual machines running compute-intensive tasks such as using CAD applications, playing HD videos, or driving 4K display resolutions.
- Two virtual CPUs are generally recommended for other cases.

Because many virtual machines run on one server, CPU can spike if agents such as antivirus agents all check for updates at exactly the same time. Determine which agents and how many agents could cause performance issues and adopt a strategy for addressing these issues. For example, the following strategies might be helpful in your enterprise:

- Use instant-clone desktop pools instead of desktop pools of full virtual machines for your virtual desktops. With instant clones, you can patch the golden image and then use push image to propagate the patch on a rolling basis across your pool of desktops. This eliminates the software update bottleneck typically associated with traditional patch management software that downloads and updates patch directly on each individual virtual desktop.
- Schedule antivirus and software updates to run at non-peak hours, when few users are likely to be logged in.
- Stagger or randomize when updates occur.
- Use agent-less antivirus software that is compatible with the VMware NSX Guest Introspection capabilities.

As an informal initial sizing approach, to start, assume that each virtual machine requires 1/8 to 1/10 of a CPU core as the minimum guaranteed compute power. That is, plan a pilot that uses 8 to 10 virtual machines per core. For example, if you assume 8 virtual machines per core and have a 2-socket 8-core ESXi host, you can host 128 virtual machines on the server during the pilot. Monitor the overall CPU usage on the host during this period and ensure that it rarely exceeds a safety margin such as 80 percent to give enough headroom for spikes.

Choosing the Appropriate System Disk Size

When allocating disk space, provide only enough space for the operating system, applications, and additional content that users might install or generate. Usually this amount is smaller than the size of the disk that is included on a physical PC.

Because data center disk space usually costs more per gigabyte than desktop or laptop disk space in a traditional PC deployment, optimize the operating system image size. The following suggestions might help optimize image size:

- Remove unnecessary files. For example, reduce the quotas on temporary internet files.

- Turn off Windows services such as the indexer service, the defragmenter service, and restore points. For details, see the *Setting Up Virtual Desktops in Horizon* document.
- Choose a virtual disk size that is sufficient to allow for future growth, but is not unrealistically large.
- Use centralized file shares or App Volumes for user-generated content and user-installed applications.
- Enable space reclamation for vCenter Server to automatically reclaim space used by stale or deleted data within a guest operating system.

The amount of storage space required must take into account the following files for each virtual desktop:

- The ESXi suspend file is equivalent to the amount of RAM allocated to the virtual machine.
- By default, the Windows page file is equivalent to 150 percent of RAM.
- Log files can take up as much as 100MB for each virtual machine.
- The virtual disk, or `.vmdk` file, must accommodate the operating system, applications, and future applications and software updates. The virtual disk must also accommodate local user data and user-installed applications if they are located on the virtual desktop rather than on file shares.

  If you use instant clones, the `.vmdk` files grow over time within a login session. Whenever a user logs out, the instant clone desktop is automatically deleted and a new instant clone is created and ready for the next user to log in. With this process, the desktop is effectively refreshed and returned to its original size.

You can also add 15 percent to this estimate to be sure that users do not run out of disk space.

Desktop Virtual Machine Configuration

The example settings for items such as memory, number of virtual processors, and disk space are specific to VMware Horizon.

The amount of system disk space required depends on the number of applications required in the base image. VMware has validated a setup that included 8GB of disk space. Applications included Microsoft Word, Excel, PowerPoint, Adobe Reader, Internet Explorer,McAfee Antivirus, and PKZIP.

The amount of disk space required for user data depends on the role of the end user and organizational policies for data storage.

The guidelines listed in the following table are for a standard Windows 10 virtual machine desktop.

Table 4-2. Desktop Virtual Machine Example for Windows 10

Item	Example
Operating system	Windows 10 (with the latest service pack)
RAM	4GB
Virtual CPU	2
System disk capacity	24GB (slightly less than standard)
Virtual SCSI adapter type	Select either LSI Logic SAS or VMware Paravirtual (PVSCSI). Using PVSCSI may require additional steps depending on the version of Windows to be installed. For more information, see the VMware Knowledge Base article Configuring disks to use VMware Paravirtual SCSI (PVSCSI) controllers (1010398).
Virtual network adapter	VMXNET 3

RDS Host Virtual Machine Configuration

Use RDS (Remote Desktop Services) hosts for providing published applications and session-based remote desktops to end users.

An RDS host can be a physical machine or a virtual machine. This example uses a virtual machine with the specifications listed in the following table. The ESXi host for this virtual machine can be part of a VMware HA cluster to guard against physical server failures.

Table 4-3. RDS Host Virtual Machine Example

Item	Example
Operating system	64-bit Windows Server 2012 R2
RAM	24GB
Virtual CPU	4
System disk capacity	40GB
Virtual SCSI adapter type	Select either LSI Logic SAS or VMware Paravirtual (PVSCSI). Using PVSCSI may require additional steps depending on the version of Windows to be installed. For more information, see the VMware Knowledge Base article Configuring disks to use VMware Paravirtual SCSI (PVSCSI) controllers (1010398).
Virtual network adapter	VMXNET 3

Table 4-3. RDS Host Virtual Machine Example (continued)

Item	Example
1 NIC	1 Gigabit
Maximum number of client connections total (including session-based remote desktop connections and published application connections)	50

Note If you configure RDS hosts at the lower end of the resource specifications, you might encounter resource constraints when using all features instead of the default installation.

ESXi Node

A node is a single VMware ESXi host that hosts virtual machine desktops in a VMware Horizon deployment.

VMware Horizon is most cost-effective when you maximize the consolidation ratio, which is the number of virtual machines (either used as desktops or RDS hosts) hosted on an ESXi host. The consolidation ratio is generally determined by how much CPU, RAM, and storage is available for the ESXi host, and how much is required per virtual machine while accounting for the overhead resources required for infrastructure components. Although many factors affect server selection, if you are optimizing strictly for acquisition price, you must find server configurations that have an appropriate balance of processing power, memory and storage. Use the following guidelines:

- As a general framework, consider compute capacity in terms of 8 to 10 virtual desktops per CPU core. For information about calculating CPU requirements for each virtual machine, see Estimating CPU Requirements for Virtual Machine Desktops.
- Think of memory capacity in terms of virtual desktop RAM and host RAM. For information about calculating the amount of RAM required per virtual machine, see Estimating Memory Requirements for Virtual Machine Desktops.

  Note that physical RAM costs are not linear and that in some situations, it can be cost-effective to purchase more smaller servers that do not use expensive DIMM chips. In other cases, rack density, storage connectivity, manageability and other considerations can make minimizing the number of servers in a deployment a better choice.
- In VMware Horizon, the View Storage Accelerator feature is turned on by default, which allows ESXi hosts to cache common virtual machine disk data. View Storage Accelerator can improve performance and reduce the need for extra storage I/O bandwidth to manage boot storms and anti-virus scanning I/O storms. This feature requires up to 32GB of RAM per ESXi host. For more information about View Storage Accelerator, see "Configuring View Storage Accelerator for vCenter Server" in the *Horizon Installation* document.
- Finally, consider cluster requirements and any failover requirements. For more information about determining requirements for high availability on vSphere clusters, see Determining Requirements for High Availability.

There is no substitute for measuring performance under actual, real world scenarios, such as in a pilot, to determine an appropriate consolidation ratio for your environment and hardware configuration. Consolidation ratios can vary significantly, based on usage patterns and environmental factors. For information about specifications of ESXi hosts in vSphere, see the *VMware vSphere Configuration Maximums* document.

vCenter Server Virtual Machine Configuration

When you deploy VMware Horizon in a vSphere environment, you will need to deploy and configure vCenter Server.

You can install vCenter Server on the same cluster of ESXi hosts that your Horizon infrastructure and workloads will run on, or on a different cluster. For information on sizing the vCenter Server based on the expected number of virtual machines it will manage, see Hardware Requirements for the vCenter Server Appliance.

Horizon Connection Server Maximums and Configuration

Horizon Connection Server can be installed either on a physical server or in a virtual machine.

Connection Server Configuration Example

This example uses a virtual machine with the specifications listed in Connection Server Virtual Machine Example. The ESXi host for this virtual machine can be part of a VMware HA cluster to guard against physical server failures.

Table 4-4. Connection Server Virtual Machine Example

Item	Example
Operating system	See supported operating systems in the *Horizon Installation* document.
RAM	10GB
Virtual CPU	4
System disk capacity	70GB
Virtual SCSI adapter type	Select either LSI Logic SAS or VMware Paravirtual (PVSCSI). Using PVSCSI may require additional steps depending on the version of Windows to be installed. For more information, see the VMware Knowledge Base article Configuring disks to use VMware Paravirtual SCSI (PVSCSI) controllers (1010398).
Virtual network adapter	VMXNET 3
Network adapter	1Gbps NIC

Connection Server Cluster Design Considerations

You can deploy multiple replicated Connection Server instances in a group to support load balancing and high availability. Groups of replicated instances are designed to support clustering within a LAN-connected single-data-center environment.

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 Horizon deployment needs to span data centers, you must use the Cloud Pod Architecture feature. For more information, see the *Administering Cloud Pod Architecture in Horizon* document.

Maximum Connections for Connection Server

The VMware Knowledge Base (KB) article https://kb.vmware.com/s/article/2150348 provides information about the tested limits regarding the number of simultaneous connections that a VMware Horizon deployment can accommodate.

PCoIP Secure Gateway connections are required if you use Unified Access Gateway appliances for PCoIP connections from outside the corporate network. Blast Secure Gateway connections are required if you use Unified Access Gateway appliances for Blast Extreme or HTML Access connections from outside the corporate network. Tunneled connections are required if you use Unified Access Gateway appliances for RDP connections from outside the corporate network and for USB and multimedia redirection (MMR) acceleration with a PCoIP or Blast Secure Gateway connection.

Although the Unified Access Gateway appliance can support a maximum of 2,000 simultaneous connections, you might choose to use 2 or 4. The required amount of memory and CPU usage might dictate that you add more Unified Access Gateway appliances per Connection Server instance to spread the load.

Although 5 Connection Server instances (suitably configured) could handle 20,000 connections, you may want to consider using 6 or 7 Connection Servers for availability planning purposes, and to accommodate connections coming from both inside and outside of the corporate network.

For example, if you had 20,000 users, with 16,000 of them inside the corporate network, you would need 5 Connection Server instances inside the corporate network. That way, if one of the instances became unavailable, the 4 remaining instances could handle the load. Similarly, for the 4,000 connections coming from outside the corporate network, you would use 2 Connection Server instances so that if one became unavailable, you would still have one instance left that could handle the load.

These numbers assume that external connections are presented through a gateway. In this example, each of the Connection Server instances handling external connections would be paired with 3 Unified Access Gateway appliances, load balanced across both Connection Server instances, so that if one became unavailable, the 2 remaining appliances could handle the load.

In all cases, users would need to reconnect if they were using a Connection Server or gateway that became unavailable.

Hardware Requirements for Unified Access Gateway with VMware Horizon

VMware recommends to use 2 vCPUs and 4GB RAM for Unified Access Gateway appliances to support maximum number of connections when used with VMware Horizon.

Table 4-5. Hardware Requirements for Unified Access Gateway

Item	Example
Operating system	OVA
RAM	4GB
Virtual CPU	2
System disk capacity	20GB (changing the default log level requires additional space)
Virtual SCSI adapter type	LSI Logic Parallel (the default for OVA)
Virtual network adapter	VMXNET 3
Network adapter	1Gbps NIC
Network Mapping	Single NIC option

vSphere Clusters

VMware Horizon deployments can use VMware HA clusters to guard against physical server failures.

vSphere and vCenter Server provide a rich set of features for managing clusters of servers that host virtual machine desktops. The cluster configuration is also important because each virtual machine desktop pool must be associated with a vCenter Server resource pool. Therefore, the maximum number of desktops per pool is related to the number of servers and virtual machines that you plan to run per cluster.

In very large VMware Horizon deployments, vCenter Server performance and responsiveness can be improved by having only one cluster object per data center object, which is not the default behavior. By default, vCenter Server creates new clusters within the same data center object.

Note For the latest updates to the VMware Horizon sizing limits and recommendations, see the VMware Knowledge Base (KB) article https://kb.vmware.com/s/article/2150348.

For more information, see the chapter about creating desktop pools, in the *Setting Up Virtual Desktops in Horizon* document. Networking requirements depend on the type of server, the number of network adapters, and the way in which VMotion is configured.

Determining Requirements for High Availability

vSphere, through its efficiency and resource management, lets you achieve industry-leading levels of virtual machines per server. But achieving a higher density of virtual machines per server means that more users are affected if a server fails.

Requirements for high availability can differ substantially based on the purpose of the desktop pool. For example, a non-persistent desktop pool might have different recovery point objective (RPO) requirements than a persistent desktop pool. For a non-persistent pool, we recommend to have users log in to a different desktop if the desktop they are using becomes unavailable.

In cases where availability requirements are high, proper configuration of VMware HA is essential. If you use VMware HA and are planning for a fixed number of desktops per server, run each server at a reduced capacity. If a server fails, the capacity of desktops per server is not exceeded when the desktops are restarted on a different host.

For example, in an 8-host cluster, where each host is capable of running 128 desktops, and the goal is to tolerate a single server failure, make sure that no more than 128 * (8 - 1) = 896 desktops are running on that cluster. You can also use VMware DRS (Distributed Resource Scheduler) to help balance the desktops among all 8 hosts. You get full use of the extra server capacity without letting any hot-spare resources sit idle. Additionally, DRS can help rebalance the cluster after a failed server is restored to service.

You must also make sure that storage is properly configured to support the I/O load that results from many virtual machines restarting at once in response to a server failure. Storage IOPS has the most effect on how quickly desktops recover from a server failure.

Storage and Bandwidth Design Considerations

Several considerations go into planning for shared storage of virtual machine desktops, planning for storage bandwidth requirements with regard to I/O storms, and planning network bandwidth needs.

- Shared Storage Considerations

  Storage design considerations are one of the most important elements of a successful VMware Horizon architecture.

- Storage Bandwidth Considerations

  In a VMware Horizon environment, logon storms are the main consideration when determining bandwidth requirements.

- Network Bandwidth Considerations

  Certain virtual and physical networking components are required to accommodate a typical workload.

Shared Storage Considerations

Storage design considerations are one of the most important elements of a successful VMware Horizon architecture.

vSphere lets you virtualize disk volumes and file systems so that you can manage and configure storage without having to consider where the data is physically stored.

Fibre Channel SAN arrays, iSCSI SAN arrays, and NAS arrays are widely used storage technologies supported by vSphere to meet different data center storage needs. The storage arrays are connected to and shared between groups of servers through storage area networks. This arrangement allows aggregation of the storage resources and provides more flexibility in provisioning them to virtual machines.

You can use VMware vSAN, which virtualizes the local physical solid-state disks and hard disk drives available on ESXi hosts into a single datastore shared by all hosts in a cluster. vSAN provides high-performance storage with policy-based management, so that you specify only one datastore when creating a desktop pool, and the various components, such as virtual machine files, replicas, user data, and operating system files, are placed on the appropriate solid-state drive (SSD) disks or direct-attached hard disks (HDDs). For more information about vSAN, see the vSphere documentation at https://docs.vmware.com/en/VMware-vSphere/index.html. For information on best practices, see the technical white paper VMware Horizon on VMware vSAN Best Practices.

For more details on storage configuration for Horizon, see "Managing Storage for Virtual Desktops" in the *Setting Up Virtual Desktops in Horizon* document.

Storage Bandwidth Considerations

In a VMware Horizon environment, logon storms are the main consideration when determining bandwidth requirements.

Although many elements are important to designing a storage system that supports a VMware Horizon environment, from a server configuration perspective, planning for proper storage bandwidth is essential. You must also consider the effects of port consolidation hardware.

VMware Horizon environments can occasionally experience I/O storm loads, during which all virtual machines undertake an activity at the same time. I/O storms can be triggered by guest-based agents such as antivirus software or software-update agents. I/O storms can also be triggered by human behavior, such as when all employees log in at nearly the same time in the morning.

You can minimize these storm workloads through operational best practices, such as staggering updates to different virtual machines. You can also test various log-off policies during a pilot phase to determine whether suspending or powering off virtual machines when users log off causes an I/O storm.

In addition to determining best practices, VMware recommends that you provide bandwidth of 1Gbps per 100 virtual machines, even though average bandwidth might be 10 times less than that. Such conservative planning guarantees sufficient storage connectivity for peak loads.

Network Bandwidth Considerations

Certain virtual and physical networking components are required to accommodate a typical workload.

For Wide-Area networks (WANs), you must consider bandwidth constraints and latency issues. The PCoIP and Blast Extreme display protocols provided by VMware adapt to varying latency and bandwidth conditions.

For display traffic, many elements can affect network bandwidth, such as protocol used, monitor resolution and configuration, and the amount of multimedia content in the workload. Concurrent launches of streamed applications can also cause usage spikes.

Because the effects of these issues can vary widely, many companies monitor bandwidth consumption as part of a pilot project. As a starting point for a pilot, plan for 150 to 200Kbps of capacity for a typical knowledge worker.

With the PCoIP or Blast Extreme display protocol, if you have an enterprise LAN with 100Mb or a 1Gb switched network, your end users can expect excellent performance under the following conditions:

- Two monitors (1920 x 1080)
- Heavy use of Microsoft Office applications
- Heavy use of Flash-embedded Web browsing
- Frequent use of multimedia with limited use of full screen mode
- Frequent use of USB-based peripherals
- Network-based printing

For more information, see the information guide called *PCoIP Display Protocol: Information and Scenario-Based Network Sizing Guide*.

Optimization Controls Available with PCoIP and Blast Extreme

If you use the PCoIP or the Blast Extreme display protocol from VMware, you can adjust several elements that affect bandwidth usage.

- You can configure the image quality level and frame rate used during periods of network congestion. The quality level setting allows you to limit the initial quality of the changed regions of the display image. You can also adjust the frame rate.

  This control works well for static screen content that does not need to be updated or in situations where only a portion needs to be refreshed.

- With regard to session bandwidth, you can configure the maximum bandwidth, in kilobits per second, to correspond to the type of network connection, such as a 4Mbit/s Internet connection. The bandwidth includes all imaging, audio, virtual channel, USB, and PCoIP or Blast control traffic.

You can also configure a lower limit, in kilobits per second, for the bandwidth that is reserved for the session, so that a user does not have to wait for bandwidth to become available. You can specify the Maximum Transmission Unit (MTU) size for UDP packets for a session, from 500 to 1500 bytes.

For more information, see the "PCoIP General Settings" and the "VMware Blast Policy Settings" sections in the *Configuring Remote Desktop Features in Horizon* document.

VMware Horizon Building Blocks

A building block is a logical construct and can contain a certain number of virtual machines. A building block consists of physical servers, a vSphere infrastructure, VMware Horizon servers, shared storage, and virtual machine desktops for end users. The scalability of each block is determined by how many virtual machines you deploy per vCenter Server.

Table 4-6. Example of a LAN-Based Horizon Building Block for 4,000 Virtual Machine Desktops

Item	Example
vSphere clusters	1
80-port network switch	1
Shared storage system	1
vCenter Server	1 (can be run in the block itself)
Database	MS SQL Server, Oracle, or PostgreSQL database server (can be run in the block itself)
VLANs	3 (a 1Gbit Ethernet network for each: management network, storage network, and VMotion network)

If you have only one building block in a pod, use two Connection Server instances for redundancy.

Horizon Pods

A Horizon pod is a unit of organization determined by VMware Horizon scalability limits. You can create a Horizon pod with a number of building blocks. Each Horizon pod is a unit of management and has a separate Horizon Console management user interface.

Pod Example Using Two Building Blocks

Table 4-7. Example of a LAN-Based Horizon Pod Constructed of 2 Building Blocks

Item	Number
Building blocks for a Horizon pod	2
vCenter Server	2
Database server	2 (1 standalone database server in each building block) MS SQL Server, Oracle, or PostgreSQL database server

Table 4-7. Example of a LAN-Based Horizon Pod Constructed of 2 Building Blocks (continued)

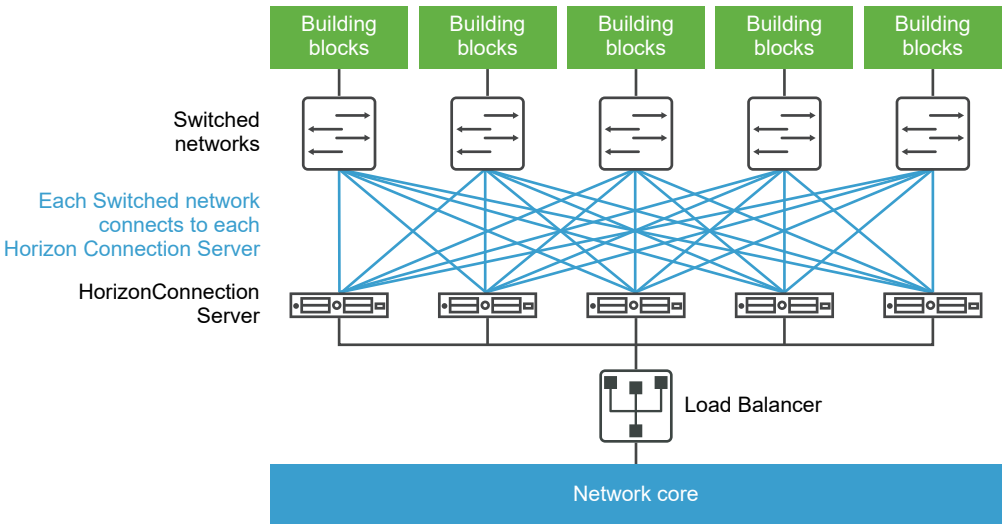
Item	Number
Connection Servers	7 (5 for connections from inside the corporate network and 2 for connections from outside)
vLANs	See Table 4-6. Example of a LAN-Based Horizon Building Block for 4,000 Virtual Machine Desktops.
10Gb Ethernet module	1
Modular networking switch	1

Depending on the specific configuration, each vCenter Server can support up a large number of virtual machines. This support enables you to have large building blocks of virtual machine desktops. However, the actual block size is also subject to other VMware Horizon-specific limitations.

For both examples described here, a network core can load balance incoming requests across Connection Server instances. Support for a redundancy and failover mechanism, usually at the network level, can prevent the load balancer from becoming a single point of failure. For example, the Virtual Router Redundancy Protocol (VRRP) can communicate with a load balancer to add redundancy and failover capability.

If a Connection Server instance fails or becomes unresponsive during an active session, users do not lose data. Desktop states are preserved in the virtual machine desktop so that users can connect to a different Connection Server instance and their desktop session resumes from where it was when the failure occurred.

Figure 4-1. Pod Diagram for Virtual Machine Desktops



Pod Example Using One vCenter Server

In the previous section, the Horizon pod consisted of multiple building blocks. Each building block supported 5,000 virtual machines with a single vCenter Server. This topic illustrates an architecture based on using a single vCenter Server to manage 10,000 desktops.

Although using one vCenter Server for 10,000 desktops is possible, doing so creates a situation where there is a single point of failure. The loss of that single vCenter Server renders the entire desktop deployment unavailable for power, provisioning, and refit operations. For this reason, choose a deployment architecture that meets your requirements for overall component resiliency.

For this example, a 10,000-user pod consists of physical servers, a vSphere infrastructure, VMware Horizon servers, shared storage, and 5 clusters of 2,000 virtual desktops per cluster.

Table 4-8. Example of a LAN-Based Horizon Pod with One vCenter Server

Item	Example
vSphere clusters	6 (5 clusters with one instant-clone pool per cluster, and 1 infrastructure cluster)
vCenter Server	1
Database server	1 (standalone) MS SQL Server, Oracle, or PostgreSQL database server
Active Directory server	1 or 2
Connection Server instances	5
Unified Access Gateway appliances	5
vLANs	8 (5 for the desktop pool clusters, and 1 each for management, VMotion, and the infrastructure cluster)

Advantages of Using Multiple vCenter Servers in a Pod

Before you attempt to manage many virtual machines with a single vCenter Server instance, you must take the following considerations into account.

- Duration of your company's maintenance windows
- Capacity for tolerating VMware Horizon component failures
- Frequency of power, provisioning, and refit operations
- Simplicity of infrastructure

Duration of Maintenance Windows

Concurrency settings for virtual machine power, provisioning, and maintenance operations are determined per vCenter Server instance.

Pod designs with one vCenter Server instance	Concurrency settings determine how many operations can be queued up for an entire Horizon pod at one time. For example, if you set concurrent provisioning operations to 20 and you have only one vCenter Server instance in a pod, a desktop pool larger than 20 will cause provisioning operations to be serialized. After queuing 20 concurrent operations simultaneously, one operation must complete before the next begins. In large-scale VMware Horizon deployments, this provisioning operation can take a long time.
Pod designs with multiple vCenter Server instances	Each instance can provision 20 virtual machines concurrently.

To ensure more operations are completed simultaneously within one maintenance window, you can add multiple vCenter Server instances (up to five) to your pod, and deploy multiple desktop pools in vSphere clusters managed by separate vCenter Server instances. A vSphere cluster can be managed by only one vCenter Server instance at one time. To achieve concurrency across vCenter Server instances, you must deploy your desktop pools accordingly.

Capacity for Tolerating Component Failures

The role of vCenter Server in Horizon pods is to provide power, provisioning, and refit (refresh, recompose, and rebalance) operations. After a virtual machine desktop is deployed and powered on, VMware Horizon does not rely on vCenter Server for the normal course of operations.

Because each vSphere cluster must be managed by a single vCenter Server instance, this server represents a single point of failure in every VMware Horizon design.

Important To use one of these failover strategies, the vCenter Server instance must not be installed in a virtual machine that is part of the cluster that the vCenter Server instance manages.

In addition to these automated options for vCenter Server failover, you can also choose to rebuild the failed server on a new virtual machine or physical server. Most key information is stored in the vCenter Server database.

Risk tolerance is an important factor in determining whether to use one or multiple vCenter Server instances in your pod design. If your operations require the ability to perform desktop management tasks such as power and refit of all desktops simultaneously, you should spread the impact of an outage across fewer desktops at a time by deploying multiple vCenter Server instances. If you can tolerate your desktop environment being unavailable for management or provisioning operations for a long period, or if you choose to use a manual rebuild process, you can deploy a single vCenter Server instance for your pod.

Frequency of Power, Provisioning, and Refit Operations

Certain virtual machine desktop power, provisioning, and refit operations are initiated only by administrator actions, are usually predictable and controllable, and can be confined to established maintenance windows. Other virtual machine desktop power and refit operations are triggered by user behavior, such as using the Refresh on Logoff or Suspend on Logoff settings, or by scripted action, such as using Distributed Power Management (DPM) during windows of user inactivity to power off idle ESXi hosts.

If your VMware Horizon design does not require user-triggered power and refit operations, a single vCenter Server instance can probably suit your needs. Without a high frequency of user-triggered power and refit operations, no long queue of operations can accumulate that might cause Horizon Connection Server to time-out waiting for vCenter Server to complete the requested operations within the defined concurrency setting limits.

Many customers elect to deploy floating pools and use the Refresh on Logoff setting to consistently deliver desktops that are free of stale data from previous sessions. Examples of stale data include unclaimed memory pages in `pagefile.sys` or Windows `temp` files. Floating pools can also minimize the impact of malware by frequently resetting desktops to a known clean state.

Some customers are reducing electricity usage by configuring VMware Horizon to power off desktops not in use so that vSphere DRS (Distributed Resources Scheduler) can consolidate the running virtual machines onto a minimum number of ESXi hosts. VMware Distributed Power Management then powers off the idle hosts. In scenarios such as these, multiple vCenter Server instances can better accommodate the higher frequency of power and refit operations required to avoid operations time-outs.

Simplicity of Infrastructure

A single vCenter Server instance in a large-scale VMware Horizon design offers some compelling benefits, such as a single place to manage golden image virtual machines, a single vCenter Server view to match the Horizon Console view, and fewer production back-end databases and database servers. Disaster Recovery planning is simpler for one vCenter Server than it is for multiple instances. Make sure you weigh the advantages of multiple vCenter Server instances, such as duration of maintenance windows and frequency of power and refit operations, against the disadvantages, such as the additional administrative overhead of managing golden image virtual machine images and the increased number of infrastructure components required.

Your design might benefit from a hybrid approach. You can choose to have very large and relatively static pools managed by one vCenter Server instance and have several smaller, more dynamic desktop pools managed by multiple vCenter Server instances. The best strategy for upgrading existing large-scale pods is to first upgrade the VMware software components of your existing pod. Before changing your pod design, gauge the impact of the improvements of the latest version's power, provisioning, and refit operations, and later experiment with increasing the size of your desktop pools to find the right balance of more large desktop pools on fewer vCenter Server instances.

Cloud Pod Architecture Overview

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

This feature uses standard Horizon components to provide cross-data-center administration, global and flexible user-to-desktop mapping, high-availability desktops, and disaster recovery capabilities.

A typical Cloud Pod Architecture topology consists of two or more pods, which are linked together in a pod federation. Pod federations are subject to certain limits. The Cloud Pod Architecture feature can be used to connect pods running on-premises, on a public cloud, or a mix of both. For more information, see the *Administering Cloud Pod Architecture in Horizon* document.

Planning for Security Features 5

VMware Horizon offers strong network security to protect sensitive corporate data. For added security, you can integrate VMware Horizon with certain third-party user-authentication solutions and implement the restricted entitlements feature.

Important VMware Horizon 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 in FIPS mode. Not all features are supported in FIPS mode. For more information, see the *Horizon Installation* document.

This chapter includes the following topics:

Understanding Client Connections

Horizon Client and Horizon Console communicate with a Horizon Connection Server host over secure HTTPS connections. Information about the server certificate on Connection Server is communicated to the client as part of the TLS handshake between client and server.

The initial Horizon Client connection, which is used for user authentication and remote desktop and application selection, is created when a user opens Horizon Client and provides a fully qualified domain name for the Connection Server or Unified Access Gateway host. The Horizon Console connection is created when an administrator types the Horizon Console URL into a web browser.

A default TLS server certificate is generated during Connection Server installation. By default, TLS clients are presented with this certificate when they visit a secure page such as Horizon Console.

You can use the default certificate for testing, but you should replace it with your own certificate as soon as possible. The default certificate is not signed by a commercial Certificate Authority (CA). Use of non-certified certificates can allow untrusted parties to intercept traffic by masquerading as your server.

- Client Connections Using the PCoIP and Blast Secure Gateways

  When clients connect to a remote desktop or application with the PCoIP or Blast Extreme display protocol from VMware, Horizon Client can make a second connection to the applicable Secure Gateway component on a Horizon Connection Server instance or Unified Access Gateway appliance. This connection provides the required level of security and connectivity when accessing remote desktops and applications from the Internet.

- Tunneled Client Connections with Microsoft RDP

  When users connect to a remote desktop with the Microsoft RDP display protocol, Horizon Client can make a second HTTPS connection to the Horizon Connection Server host. This connection is called the tunnel connection because it provides a tunnel for carrying RDP data.

- Direct Client Connections

  Administrators can configure Horizon Connection Server settings so that remote desktop and published application sessions are established directly between the client system and the published application or desktop virtual machine, bypassing the Connection Server host. This type of connection is called a direct client connection.

Client Connections Using the PCoIP and Blast Secure Gateways

When clients connect to a remote desktop or application with the PCoIP or Blast Extreme display protocol from VMware, Horizon Client can make a second connection to the applicable Secure Gateway component on a Horizon Connection Server instance or Unified Access Gateway appliance. This connection provides the required level of security and connectivity when accessing remote desktops and applications from the Internet.

Unified Access Gateway appliances include a PCoIP Secure Gateway component and a Blast Secure Gateway component, which offers the following advantages:

- The only remote desktop and application traffic that can enter the corporate data center is traffic on behalf of a strongly authenticated user.
- Users can access only the resources that they are authorized to access.
- The PCoIP Secure Gateway connection supports PCoIP, and the Blast Secure Gateway connection supports Blast Extreme. Both are advanced remote display protocols that make more efficient use of the network by encapsulating video display packets in UDP instead of TCP.
- PCoIP and Blast Extreme are secured by AES-128 encryption by default. You can, however, change the encryption cipher to AES-256.

- No VPN is required, as long as the display protocol is not blocked by any networking component. For example, someone trying to access their remote desktop or application from inside a hotel room might find that the proxy the hotel uses is not configured to pass UDP packets.

For more information about Unified Access Gateway virtual appliances, see *Deploying and Configuring VMware Unified Access Gateway*.

Tunneled Client Connections with Microsoft RDP

When users connect to a remote desktop with the Microsoft RDP display protocol, Horizon Client can make a second HTTPS connection to the Horizon Connection Server host. This connection is called the tunnel connection because it provides a tunnel for carrying RDP data.

The tunnel connection offers the following advantages:

- RDP data is tunneled through HTTPS and is encrypted using SSL. This powerful security protocol is consistent with the security provided by other secure Web sites, such as those that are used for online banking and credit card payments.
- A client can access multiple desktops over a single HTTPS connection, which reduces the overall protocol overhead.
- Because VMware Horizon manages the HTTPS connection, the reliability of the underlying protocols is significantly improved. If a user temporarily loses a network connection, the HTTP connection is reestablished after the network connection is restored and the RDP connection automatically resumes without requiring the user to reconnect and log in again.

In a standard deployment of Connection Server instances, the HTTPS secure connection terminates at the Connection Server. In a DMZ deployment, the HTTPS secure connection terminates at a Unified Access Gateway appliance.

Clients that use the PCoIP or Blast Extreme display protocol can use the tunnel connection for USB redirection and multimedia redirection (MMR) acceleration, but for all other data, PCoIP uses the PCoIP Secure Gateway, and Blast Extreme uses the Blast Secure Gateway, on a Unified Access Gateway appliance. For more information, see Client Connections Using the PCoIP and Blast Secure Gateways .

For more information about Unified Access Gateway virtual appliances, see *Deploying and Configuring VMware Unified Access Gateway*.

Direct Client Connections

Administrators can configure Horizon Connection Server settings so that remote desktop and published application sessions are established directly between the client system and the published application or desktop virtual machine, bypassing the Connection Server host. This type of connection is called a direct client connection.

With direct client connections, an HTTPS connection is still made between the client and the Connection Server host for users to authenticate and select remote desktops and published applications, but the second HTTPS connection (the tunnel connection) is not used.

Direct PCoIP and Blast Extreme connections include the following built-in security features:

- Support for Advanced Encryption Standard (AES) encryption, which is turned on by default, and IP Security (IPsec)
- Support for third-party VPN clients

For clients that use the Microsoft RDP display protocol, direct client connections to remote desktops are appropriate only if your deployment is inside a corporate network. With direct client connections, RDP traffic is sent unencrypted over the connection between the client and the desktop virtual machine.

Choosing a User Authentication Method

VMware Horizon uses your existing Active Directory infrastructure for user authentication and management. For added security, you can integrate VMware Horizon with two-factor authentication solutions, such as RSA SecurID and RADIUS, and smart card authentication solutions.

- Active Directory Authentication

  Each Horizon Connection Server instance is joined to an Active Directory domain, and users are authenticated against Active Directory for the joined domain. Users are also authenticated against any additional user domains with which a trust agreement exists.

- Using Two-Factor Authentication

  You can configure a Horizon Connection Server instance so that users are required to use RSA SecurID authentication or RADIUS (Remote Authentication Dial-In User Service) authentication.

- Smart Card Authentication

  A smart card is a small plastic card that is embedded with a computer chip. Many government agencies and large enterprises use smart cards to authenticate users who access their computer networks. One type of smart card used by the United States Department of Defense is called a Common Access Card (CAC).

- Using the Log In as Current User Feature Available with Windows-Based Horizon Client

  With Horizon Client for Windows, when users select **Log in as current user** in the **Options** menu, the credentials that they provided when logging in to the client system are used to authenticate to the Horizon Connection Server instance and to the remote desktop using Kerberos. No further user authentication is required.

Active Directory Authentication

Each Horizon Connection Server instance is joined to an Active Directory domain, and users are authenticated against Active Directory for the joined domain. Users are also authenticated against any additional user domains with which a trust agreement exists.

For example, if a Connection Server instance is a member of Domain A and a trust agreement exists between Domain A and Domain B, users from both Domain A and Domain B can connect to the Connection Server instance with Horizon Client.

Similarly, if a trust agreement exists between Domain A and an MIT Kerberos realm in a mixed domain environment, users from the Kerberos realm can select the Kerberos realm name when connecting to the Connection Server instance with Horizon Client.

You can place 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

Connection Server determines which domains are accessible by traversing trust relationships, starting with the domain in which the host resides. For a small, well-connected set of domains, Connection Server can quickly determine a 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 log in to their remote desktops and applications.

Administrators can use the `vdmadmin` command-line interface to configure domain filtering, which limits the domains that a Connection Server instance searches and that it displays to users. See the *Horizon Administration* document for more information.

Policies, such as restricting permitted hours to log in and setting the expiration date for passwords, are also handled through existing Active Directory operational procedures.

Using Two-Factor Authentication

You can configure a Horizon Connection Server instance so that users are required to use RSA SecurID authentication or RADIUS (Remote Authentication Dial-In User Service) authentication.

- RADIUS support offers a wide range of alternative two-factor token-based authentication options.
- VMware Horizon also provides an open standard extension interface to allow third-party solution providers to integrate advanced authentication extensions into VMware Horizon.

Because two-factor authentication solutions such as RSA SecurID and RADIUS work with authentication managers, installed on separate servers, you must have those servers configured and accessible to the Connection Server host. For example, if you use RSA SecurID, the authentication manager would be RSA Authentication Manager. If you have RADIUS, the authentication manager would be a RADIUS server.

To use two-factor authentication, each user must have a token, such as an RSA SecurID token, that is registered with its authentication manager. A two-factor authentication token is a piece of hardware or software that generates an authentication code at fixed intervals. Often authentication requires knowledge of both a PIN and an authentication code.

If you have multiple Connection Server instances, you can configure two-factor authentication on some instances and a different user authentication method on others. For example, you can configure two-factor authentication only for users who access remote desktops and applications from outside the corporate network, over the Internet.

VMware Horizon is certified through the RSA SecurID Ready program and supports the full range of SecurID capabilities, including New PIN Mode, Next Token Code Mode, RSA Authentication Manager, and load balancing.

Smart Card Authentication

A smart card is a small plastic card that is embedded with a computer chip. Many government agencies and large enterprises use smart cards to authenticate users who access their computer networks. One type of smart card used by the United States Department of Defense is called a Common Access Card (CAC).

Administrators can enable individual Connection Server instances for smart card authentication. Enabling a Connection Server instance to use smart card authentication typically involves adding your root certificate to a truststore file and then modifying Connection Server settings.

All client connections, including client connections that use smart card authentication, are TLS/SSL enabled.

To use smart cards, client machines must have smart card middleware and a smart card reader. To install certificates on smart cards, you must set up a computer to act as an enrollment station. For information about whether a particular type of Horizon Client supports smart cards, see the Horizon Client documentation at https://docs.vmware.com/en/VMware-Horizon-Client/index.html.

Using the Log In as Current User Feature Available with Windows-Based Horizon Client

With Horizon Client for Windows, when users select **Log in as current user** in the **Options** menu, the credentials that they provided when logging in to the client system are used to authenticate to the Horizon Connection Server instance and to the remote desktop using Kerberos. No further user authentication is required.

To support this feature, user credentials are stored on both the Connection Server instance and on the client system.

- On the Connection Server instance, user credentials are encrypted and stored in the user session along with the username, domain, and optional UPN. The credentials are added when authentication occurs and are purged when the session object is destroyed. The session object is destroyed when the user logs out, the session times out, or authentication fails. The session object resides in volatile memory and is not stored in Horizon LDAP or in a disk file.
- On the Connection Server instance, enable the **Accept logon as current user** setting to allow the Connection Server instance to accept the user identity and credential information that is passed when users select **Log in as current user** in the **Options** menu in Horizon Client.

  Important You must understand the security risks before enabling this setting. See, "Security-Related Server Settings for User Authentication" in the *Horizon Security* document.

- On the client system, user credentials are encrypted and stored in a table in the Authentication Package, which is a component of Horizon Client. The credentials are added to the table when the user logs in and are removed from the table when the user logs out. The table resides in volatile memory.

  When you select **Accept logon as current user**, you can enable the following user settings:

  - Allow Legacy Clients: Support for older clients. Horizon Client versions 2006 and 5.4 and earlier versions are considered older clients.
  - Allow NTLM Fallback: Uses NTLM authentication instead of Kerberos when there is no access to the domain controller. The NTLM group policy settings must be enabled in Horizon Client configuration.
  - Disable Channel Bindings: An additional security layer to secure NTLM authentication. By default, channel bindings are enabled on the client.
  - True SSO Integration: Enable this setting on Connection Server to allow SSO to the desktop using True SSO. For example, in a nested mode, True SSO is used to log on to a nested client and then a secondatry desktop logon was performed. For information on nested mode, see the *VMware Horizon Client for Windows Installation and Setup Guide*.
    - Disabled: The user has to enter login information if the client did not receive logon credentials.
    - Optional: Client credentials will be used, if available, else True SSO will be used. This is the recommended setting if both True SSO and Log in as current user are enabled.
    - Enabled: True SSO will be used to log on to the desktop.

Administrators can use Horizon Client group policy settings to control the availability of the **Log in as current user** setting in the **Options** menu and to specify its default value. Administrators can also use group policy to specify which Connection Server instances accept the user identity and credential information that is passed when users select **Log in as current user** in Horizon Client.

The Recursive Unlock feature is enabled after a user logs in to Connection Server with the Log in as current user feature. The Recursive Unlock feature unlocks all remote sessions after the client machine has been unlocked. Administrators can control the Recursive Unlock feature with the **Unlock remote sessions when the client machine is unlocked** global policy setting in Horizon Client. For more information about global policy settings for Horizon Client, see the Horizon Client documentation at the VMware Horizon Clients documentation Web page.

Note The Recursive Unlock feature may be slow when you use Log in as current user with NTLM authentication if Horizon Client is unable to access the domain controllers. To mitigate this issue, enable the group policy setting **Always use NTLM for servers** in the **VMware Horizon Client Configuration > Security Settings > NTLM Settings** folder in the Group Policy Management Editor.

The Log in as current user feature has the following limitations and requirements:

- When smart card authentication is set to Required on a Connection Server instance, authentication fails for users who select **Log in as current user** when they connect to the Connection Server instance. These users must reauthenticate with their smart card and PIN when they log in to Connection Server.
- The time on the system where the client logs in and the time on the Connection Server host must be synchronized.
- If the default **Access this computer from the network** user-right assignments are modified on the client system, they must be modified as described in VMware Knowledge Base (KB) article 1025691.

Restricting Remote Desktop Access

You can use the restricted entitlements feature to restrict remote desktop access based on the Horizon Connection Server instance that a user connects to.

With restricted entitlements, you assign one or more tags to a Connection Server instance. Then, when configuring a desktop pool, you select the tags of the Connection Server instances that you want to be able to access the desktop pool. When users log in through a tagged Connection Server instance, they can access only those desktop pools that have at least one matching tag or no tags.

For example, your VMware Horizon deployment might include two Connection Server instances. The first instance supports your internal users. The second instance is paired with an Unified Access Gateway appliance and supports your external users. To prevent external users from accessing certain desktops, you could set up restricted entitlements as follows:

- Assign the tag "Internal" to the Connection Server instance that supports your internal users.
- Assign the tag "External" to the Connection Server instance that is paired with the Unified Access Gateway appliance and supports your external users.
- Assign the "Internal" tag to the desktop pools that should be accessible only to internal users.

- Assign the "External" tag to the desktop pools that should be accessible only to external users.

External users cannot see the desktop pools tagged as Internal because they log in through the Connection Server tagged as External, and internal users cannot see the desktop pools tagged as External because they log in through the Connection Server tagged as Internal.

You can also use restricted entitlements to control desktop access based on the user-authentication method that you configure for a particular Connection Server instance. For example, you can make certain desktop pools available only to users who have authenticated with a smart card.

The restricted entitlements feature only enforces tag matching. You must design your network topology to force certain clients to connect through a particular Connection Server instance.

Using Group Policy Settings to Secure Remote Desktops and Applications

VMware Horizon includes Group Policy administrative ADMX templates that contain security-related group policy settings that you can use to secure your remote desktops and applications.

For example, you can use group policy settings to perform the following tasks.

- Specify the Connection Server instances that can accept user identity and credential information that is passed when a user selects the **Log in as current user** check box in Horizon Client for Windows.
- Enable single sign-on for smart card authentication in Horizon Client.
- Configure server TLS certificate checking in Horizon Client.
- Prevent users from providing credential information with Horizon Client command line options.
- Prevent non-Horizon Client systems from using RDP to connect to remote desktops. You can set this policy so that connections must be Horizon Client-managed, which means that users must use VMware Horizon to connect to remote desktops.

See the *Configuring Remote Desktop Features in Horizon* document for information on using remote desktop and Horizon Client group policy settings.

Using Smart Policies

You can use Smart Policies for user environment settings in a published desktop or application and also for computer environment settings that apply during computer boot or session reconnection.

You can create policies for user environment settings that control a range of behaviors. Horizon Smart Policies for user environment settings are applied during login and can be refreshed during reconnect of a session. To reapply Horizon Smart Policies when a user reconnects to a session, you can configure a triggered task.

You can create policies for computer environment settings that Dynamic Environment Manager applies while end users' computers boot. Horizon Smart Policies for computer environment settings are applied during computer boot and can be refreshed during the reconnection of a session.

With Smart Policies, you can create policies that take effect only if certain conditions are met. For example, you can configure a policy that disables the client drive redirection feature if a user connects to a remote desktop from outside your corporate network.

The Smart Policies feature requires Dynamic Environment Manager. For more information, see the topics about Smart Policies in *Configuring Remote Desktop Features in Horizon*.

For information about using Smart Policies to control the behavior of features on a remote Linux desktop, see *Setting Up Linux Desktops in Horizon*.

Implementing Best Practices to Secure Client Systems

Implement these best practices to secure client systems.

- Configure client systems to go to sleep after a period of inactivity and require users to enter a password before the computer awakens.
- Require users to enter a username and password when starting client systems. Do not configure client systems to allow automatic logins.
- For Mac client systems, consider setting different passwords for the Keychain and the user account. When the passwords are different, users are prompted before the system enters any passwords on their behalf. Also consider turning on FileVault protection.

For a concise reference to all the security features VMware Horizon provides, see the *Horizon Security* document.

Assigning Administrator Roles

A key management task in a VMware Horizon environment is to determine who can use Horizon Console and what tasks those users are authorized to perform.

The authorization to perform tasks in Horizon Console is governed by an access control system that consists of administrator roles and privileges. A role is a collection of privileges. Privileges grant the ability to perform specific actions, such as entitling a user to a desktop pool or changing a configuration setting. Privileges also control what an administrator can see in Horizon Console.

An administrator can create folders to subdivide desktop pools and delegate the administration of specific desktop pools to different administrators in Horizon Console. An administrator configures administrator access to the resources in a folder by assigning a role to a user on that folder. Administrators can only access the resources that reside in folders for which they have assigned roles. The role that an administrator has on a folder determines the level of access that the administrator has to the resources in that folder.

Horizon Console includes a set of predefined roles. Administrators can also create custom roles by combining selected privileges.

Understanding Communications Protocols

VMware Horizon components use several different protocols to exchange messages.

The following table lists the default ports that each protocol uses. You can change the port numbers. For example, you might need to change the port numbers to comply with organization policies, or to avoid contention.

Table 5-1. Default Ports

Protocol	Port
JMS	TCP port 4001 TCP port 4002
HTTP	TCP port 80
HTTPS	TCP port 443
MMR/CDR	TCP port 9427 The following features use this port. ■ Windows multimedia redirection ■ Client drive redirection ■ Microsoft Teams optimization ■ HTML multimedia redirection ■ VMware printer redirection ■ USB redirection
RDP	TCP port 3389 **Note** If the Connection Server instance is configured for direct client connections, these protocols connect directly from the client to the remote desktop and are not tunneled through the Horizon Secure Gateway Server component.
SOAP	TCP port 80 or 443
PCoIP	TCP port 4172 UDP ports 4172, 50002, 55000
USB redirection	TCP port 32111. This port is also used for time zone synchronization.
VMware Blast Extreme	TCP ports 8443, 22443 UDP ports 443, 8443, 22443
HTML Access	TCP ports 8443, 22443

TCP Ports for Connection Server Intercommunication

Connection Server instances in a group use additional TCP ports to communicate with each other. For example, Connection Server instances use port 4100 or 4101 to transmit JMS inter-router (JMSIR) traffic to each other. Firewalls are typically not used between the Connection Server instances in a group.

Horizon Security Gateway

Horizon Security Gateway is the server-side component for the secure HTTPS connection between client systems and an Unified Access Gateway appliance, or Connection Server instance.

When you configure the tunnel connection for Connection Server, RDP, USB, and Multimedia Redirection (MMR) traffic is tunneled through the Horizon Security Gateway component. When you configure direct client connections, these protocols connect directly from the client to the remote desktop and are not tunneled through the Horizon Security Gateway component.

Note Clients that use the PCoIP or Blast Extreme display protocol can use the tunnel connection for USB redirection and multimedia redirection (MMR) acceleration, but for all other data, PCoIP uses the PCoIP Secure Gateway, and Blast Extreme uses the Blast Secure Gateway, on an Unified Access Gateway appliance.

Horizon Security Gateway is also responsible for forwarding other web traffic, including user authentication and desktop and application selection traffic, from clients to Connection Server. Horizon Security Gateway also passes Horizon Console client web traffic to the Horizon Administration component.

Blast Secure Gateway

Unified Access Gateway appliances include a Blast Secure Gateway component. When the Blast Secure Gateway is enabled, after authentication, clients that use Blast Extreme or HTML Access can make another secure connection to an Unified Access Gateway appliance. This connection allows clients to access remote desktops and applications from the Internet.

When you enable the Blast Secure Gateway component, Blast Extreme traffic is forwarded by an Unified Access Gateway appliance to remote desktops and applications. If clients that use Blast Extreme also use the USB redirection feature or multimedia redirection (MMR) acceleration, you can enable the View Secure Gateway component to forward that data.

When you configure direct client connections, Blast Extreme traffic and other traffic goes directly from a client to a remote desktop or application.

When end users such as home or mobile workers access desktops from the internet, Unified Access Gateway appliances provide the required level of security and connectivity so that a VPN connection is not necessary. The Blast Secure Gateway component ensures that the only remote traffic that can enter the corporate data center is traffic on behalf of a strongly authenticated user. End users can access only the resources that they are authorized to access.

A Blast native client that operates through a Blast Secure Gateway expects to have its Blast session TLS connection authenticated by the TLS certificate that is configured on the Blast Secure Gateway. If the client's Blast connection sees some other TLS certificate then the connection will be dropped and the client will report a certificate thumbprint mismatch.

If you choose to have the client make its connection to a TLS-terminating proxy placed between the client and the Blast Secure Gateway, you may satisfy the client's certificate requirement and avoid a thumbprint mismatch error by arranging for the proxy to present a copy of the Blast Secure Gateway's certificate (and private key), thereby allowing the Blast connection from the client to succeed.

An alternative to copying the Blast Secure Gateway's certificate to the proxy is to provide the proxy with its own TLS certificate, and then configure the Blast Secure Gateway to advise the client to expect and accept the proxy's certificate rather than the Blast Secure Gateway's certificate.

You can configure the Blast Secure Gateway in a Unified Access Gateway by uploading the proxy's certificate in **Blast Proxy Certificate** in the Unified Access Gateway Horizon settings. See the *Deploying and Configuring VMware Unified Access Gateway* document in https://docs.vmware.com/en/Unified-Access-Gateway/index.html.

Note Only the proxy certificate is uploaded. The corresponding private key is not disclosed to the Unified Access Gateway.

PCoIP Secure Gateway

Unified Access Gateway appliances include a PCoIP Secure Gateway component. When the PCoIP Secure Gateway is enabled, after authentication, clients that use PCoIP can make another secure connection to an Unified Access Gateway appliance. This connection allows clients to access remote desktops and applications from the internet.

When you enable the PCoIP Secure Gateway component, PCoIP traffic is forwarded by an Unified Access Gateway appliance to remote desktops and applications. If clients that use PCoIP also use the USB redirection feature or multimedia redirection (MMR) acceleration, you can enable the Horizon Security Gateway component in order to forward that data.

When you configure direct client connections, PCoIP traffic and other traffic goes directly from a client to a remote desktop or application.

When end users such as home or mobile workers access desktops from the internet, Unified Access Gateway appliances provide the required level of security and connectivity so that a VPN connection is not necessary. The PCoIP Secure Gateway component ensures that the only remote traffic that can enter the corporate data center is traffic on behalf of a strongly authenticated user. End users can access only the resources that they are authorized to access.

Horizon LDAP

Horizon LDAP is an embedded LDAP directory in Connection Server and is the configuration repository for all VMware Horizon configuration data.

Horizon LDAP contains entries that represent each remote desktop and application, each accessible remote desktop, multiple remote desktops that are managed together, and VMware Horizon component configuration settings.

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

Horizon Messaging

The Horizon Messaging component provides the messaging router for communication between Horizon Connection Server components and between Horizon Agent and Connection Server.

This component supports the Java Message Service (JMS) API, which is used for messaging in VMware Horizon.

Intercomponent message validation uses DSA keys. The key size is 512 bits by default, except in FIPS mode, where the key size is 2048 bits.

Firewall Rules for Horizon Connection Server

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

When you install Connection Server, the installation program 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 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 5-2. 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
PCoIP	TCP 4172 in; UDP 4172 both directions	Standard, replica

Table 5-2. Ports Opened During Horizon Connection Server Installation (continued)

Protocol	Ports	Horizon Connection Server Instance Type
HTTPS	TCP 8443 UDP 8443	Standard, replica After the initial connection to VMware Horizon 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 interpod 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.

Firewall Rules for Horizon Agent

To open the default network ports, the Horizon Agent installer optionally configures Windows firewall rules on virtual desktops and RDS hosts.

The Horizon Agent installer configures the local firewall rule for inbound RDP connections to match the current RDP port of the host operating system, which is typically 3389.

If you instruct the Horizon Agent installer not to enable Remote Desktop support, it does not open ports 3389 and 32111 and you must open these ports manually.

If you change the RDP port number after installation, you must change the associated firewall rules. If you change a default port after installation, you must manually reconfigure the firewall rules to allow access on the updated port. For more information, see the *Horizon Installation* document.

On RDS hosts, the Windows firewall rules for Horizon Agent show a block of 256 contiguous UDP ports as open for inbound traffic. This block of ports is for VMware Blast internal use in Horizon Agent. A special Microsoft-signed driver on RDS hosts blocks inbound traffic to these ports from external sources. This driver causes the Windows firewall to treat the ports as closed.

If you use a virtual machine template as a desktop source, firewall exceptions carry over to deployed desktops only if the template is a member of the desktop domain. You can use Microsoft group policy settings to manage local firewall exceptions. For more information, see Microsoft Knowledge Base (KB) article 875357.

The following table lists the TCP and UDP ports that are opened during Horizon Agent installation. Ports are incoming unless otherwise noted.

Table 5-3. TCP and UDP Ports Opened During Horizon Agent Installation

Protocol	Ports
RDP	TCP port 3389
USB redirection and time zone synchronization	TCP port 32111
Multimedia redirection (MMR) and client drive redirection (CDR)	TCP port 9427 The following features use this port: ■ Windows multimedia redirection ■ Client drive redirection ■ Microsoft Teams optimization ■ HTML multimedia redirection ■ VMware printer redirection ■ USB redirection
PCoIP	For RDS hosts, PCoIP uses TCP port 4172 and UDP port 4172 (bidirectional). For virtual desktops, PCoIP uses port numbers selected from a configurable range. By default, PCoIP uses TCP ports 4172 to 4173 and UDP ports 4172 to 4182. The firewall rules do not specify port numbers. Instead, they dynamically follow the ports opened by each PCoIP server. The selected port numbers are communicated to the client through the Connection Server instance.
VMware Blast	TCP port 22443 UDP port 22443 (bidirectional) **Note** UDP is not used on Linux desktops.
HTML Access	TCP port 22443
XDMCP	UDP 177 **Note** This port is opened for XDMCP access only on Linux desktops running Ubuntu 18.04. Firewall rules block all external host access to this port.
X11	TCP 6100 **Note** This port is opened for XServer access only on Linux desktops running Ubuntu 18.04. Firewall rules block all external host access to this port.

Firewall Rules for Active Directory

If you have a firewall between your VMware Horizon environment and your Active Directory server, you must make sure that all of the necessary ports are opened.

For example, Connection Server must be able to access the Active Directory Global Catalog and Lightweight Directory Access Protocol (LDAP) servers. If the Global Catalog and LDAP ports are blocked by your firewall software, administrators will have problems configuring user entitlements.

See the Microsoft documentation for your Active Directory server version for information about the ports that must be opened for Active Directory to function correctly through a firewall.

Overview of Steps to Setting Up a VMware Horizon Environment

6

Complete these high-level tasks to install VMware Horizon and configure an initial deployment.

Table 6-1. VMware Horizon Installation and Setup Check List

Step	Task
1	Set up the required administrator users and groups in Active Directory. Instructions: *Horizon Installation* and vSphere documentation.
2	If you have not yet done so, install and set up ESXi hosts and vCenter Server. Instructions: VMware vSphere documentation.
4	Install and set up Horizon Connection Server. Also install the Events database. Instructions: *Horizon Installation* document.
5	Create one or more virtual machines that can be used as a template for full-clone desktop pools or as a parent for instant-clone desktop pools. Instructions: *Setting Up Virtual Desktops in Horizon*.
6	(Optional) Set up an RDS host and install applications to be remoted to end users. Instructions: *Setting Up Published Desktops and Applications in Horizon*.
7	Create virtual and published desktop pools, application pools, or both. Instructions: *Setting Up Virtual Desktops in Horizon* and *Setting Up Published Desktops and Applications in Horizon*.
8	Control user access to desktops. Instructions: *Configuring Remote Desktop Features in Horizon*.
9	Install Horizon Client on end users' machines and have end users access their remote desktops and applications. Instructions: Horizon Client documentation at https://docs.vmware.com/en/VMware-Horizon-Client/index.html.
10	(Optional) Create and configure additional administrators to allow different levels of access to specific inventory objects and settings. Instructions: *Horizon Administration* document.
11	(Optional) Configure policies to control the behavior of VMware Horizon components, desktop and application pools, and end users. Instructions: *Configuring Remote Desktop Features in Horizon*.
13	(Optional) For added security, integrate smart card authentication or a RADIUS two-factor authentication solution. Instructions: *Horizon Administration* document.