REVISED 3 OCTOBER 2018

VMWARE HORIZON CLOUD SERVICE WITH HOSTED INFRASTRUCTURE DEPLOYMENT CONSIDERATIONS

vmware®

Table of Contents

Introduction

– Intended Audience

What Is the VMware Horizon Cloud Service Family?

– Horizon Cloud Service with Hosted Infrastructure

– Horizon Cloud Service Administration Console

– Service Models

– Service Description

– System Architecture

Avoiding Obstacles That Prolong the Deployment Process

– Establishing Business Drivers, Objectives, and Project Milestones

– Identifying Key Project Stakeholders

– Conducting Desktop Assessments, and Identifying Use Cases and User Communities

– Gathering Business and Technical Requirements

– Understanding the Horizon Cloud Service Deployment Process

– Identifying Key Areas of Responsibility

– Completing the Horizon Cloud-Hosted Setup Web Form

– Discussing Platform Design Considerations

– Attending the Kickoff Meeting

Choosing Strategic Network Options

– IPsec VPN, Dedicated Connections, MPLS, and Network Exchange Options

- Choosing the Ideal Type of Network Connection
- Horizon Cloud Service Network Options
- Firewall Exceptions and Required Ports
- Unified Access Gateway
- Network Routing
- IPsec VPN Parameters (Optional)

Meeting Active Directory Requirements

- Choosing an Existing or Isolated Active Directory
- Creating Service Accounts for Active Directory
- Creating Groups for Active Directory
- Creating a Unique Horizon Cloud Service OU for Active Directory
- Setting Up DHCP Scopes and Option Code 74 or Manually Configuring DaaS Agents

Creating Optimized Images

- Optimizing Your Desktop Images
- Deciding How Many Images You Need
- Using Traditional or Instant-Clone Images
- Creating Images for RDSH Servers
- Understanding Dedicated, Floating, and Session Desktops
- Choosing 3D Graphics Options
- Staggering Automatic Antivirus Updates

Assigning Applications

- Managing Remote Applications

Image Management Strategies

- Profile Management
- Patch Management
- Backup Strategies

Additional Resources

About the Authors and Contributor

Feedback

VMware Horizon Cloud Service with Hosted Infrastructure Deployment Considerations

Introduction

VMware Horizon® Cloud Service™ is a family of cloud services from VMware that enables the delivery of virtual desktops and applications to end users on any supported device. Horizon Cloud Service is available in two ways: as a VMware-hosted infrastructure or hosted in your own Microsoft Azure instance. In both scenarios, the management of the infrastructure is done by the Horizon Cloud Service application.

This document focuses on VMware Horizon Cloud Service with Hosted Infrastructure. It describes the most common issues that can arise during deployment and includes tips on how to avoid these issues in your own implementation. Although each environment is unique, the general considerations described here can assist you in most effectively deploying Horizon Cloud Service with Hosted Infrastructure.

Intended Audience

This document is for IT decision-makers, architects, administrators, and others who want to familiarize themselves with, or are in the process of, a Horizon Cloud Service with Hosted Infrastructure deployment. You should be familiar with Windows data center technologies, such as Active Directory, SQL, and Microsoft Management Console. You should also be familiar with cloud computing, site-to-site (S2S) VPNs, and Multi-Protocol Label Switching (MPLS) networks.

What Is the VMware Horizon Cloud Service Family?

Horizon Cloud Service delivers virtual desktops and applications using a purpose-built cloud platform that is scalable across multiple deployment options, including on-premises infrastructure or fully managed infrastructure from VMware. The service supports a cloud-scale architecture to deliver virtualized Windows desktops and applications to multiple devices, simplifying setup and scalability.

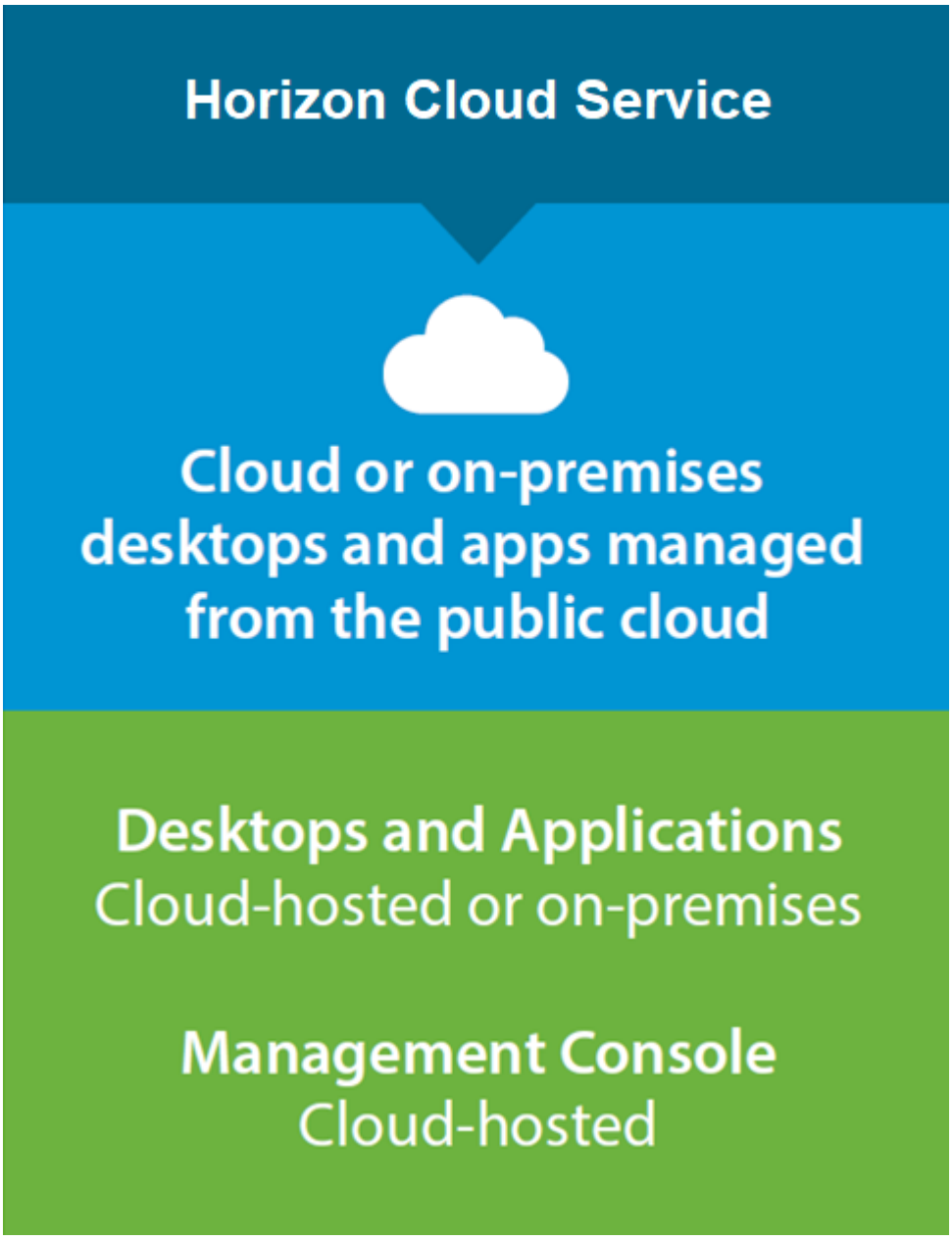

Figure 1: Horizon Cloud Service Family

Horizon Cloud Service with Hosted Infrastructure

Horizon Cloud Service with Hosted Infrastructure simplifies the delivery of Windows desktops and applications as a cloud service while maintaining enterprise requirements for security and control. End users benefit from a complete workspace that they can access from a variety of device types from almost any location. Horizon Cloud Service with Hosted Infrastructure also offers an on-demand, flexible desktop and application delivery platform that can grow or shrink based on the needs and demands of your business.

Horizon Cloud Service Administration Console

The Horizon Cloud Service Administration Console provides full life-cycle management of desktops and Remote Desktop Session Host (RDSH) through a single, easy-to-use web-based console. Organizations can securely provision and manage desktop models and entitlements, as well as native and remote applications, through the centralized Horizon Cloud Service Administration Console. The Administration Console also provides usage and activity reports for various user, administrative, and capacity-management activities.

Service Models

Horizon Cloud Service packages come in standard sizes that can be configured to meet your performance requirements. You can mix and match the desktop reservation capacity as needed to fit your enterprise. For more information, see How to Buy.

Service Description

The Service Description: VMware Horizon Cloud Service with Hosted Infrastructure document details the components, definitions, and service capabilities. It includes information on licensing, management and user portals, service offerings, and features included in the Horizon Cloud Service with Hosted Infrastructure platform. Review this document for more detailed information about the Horizon Cloud Service.

System Architecture

Horizon Cloud Service with Hosted Infrastructure consists of the following major components:

• **Image, also called image template** – A desktop or RDSH server image that can be used in a Horizon Cloud Service infrastructure to create desktop or application assignments. It is used as the base image from which virtual machines (VMs) are cloned.

• **VMware Horizon Client™** – Software-based client installed on a desktop, thin client, mobile device, or tablet that facilitates connectivity to Horizon Cloud Service–hosted desktops and applications.

• **Horizon Cloud Service tenant appliance** – A hardened Linux appliance that provides desktop and application brokering, provisioning, and entitlement services. It hosts the end-user and administrative portals.

• **Horizon Cloud Service–hosted virtual desktop** – A virtualized and optimized desktop that is hosted in Horizon Cloud Service. A virtual desktop supports a single connection, delivering a fully functional desktop to the end user. Horizon Cloud Service agents are installed on the virtual desktop to support a connection from the Horizon Client.

• **Horizon Cloud Service–hosted RDSH** – A server-based model for delivering applications and shared full desktops in Horizon Cloud Service using Microsoft Remote Desktop Services and VMware Horizon technology. Compared to a single connection for each virtual desktop, RDSH servers can support multiple desktop and application sessions from different users. Horizon Cloud Service agents are installed on the RDSH servers to support connections from the Horizon Client.

• **Desktop and services subnets** – Unique IP subnets that you assign to allow for desktop, application, and administrative connectivity. The Desktop Zone uses the desktop subnet for virtual desktops and RDSH servers. The Services Zone uses the services subnet for tenant appliances and other utility services.

• **Horizon Cloud Service User Portal** – A web-based portal offering users clientless access to Horizon Cloud Service desktops and applications using HTML5.

• **Horizon Cloud Service Administration Console** – The web-based portal used by IT administrators to provision and manage Horizon Cloud Service desktops and applications, resource entitlements, and images.

• **Edge Gateway** – A gateway that provides network edge security and gateway services to isolate security zones and virtualized networks along with NAT, DHCP, VPN, and a load balancer.

• **VMware Unified Access Gateway** – A hardened Linux appliance that allows for secure remote access into the Horizon Cloud Service environment and is part of the Security Zone (for external Horizon Cloud Service access) and the Services Zone (for internal Horizon Cloud Service access).

For additional terms and concepts, see the VMware Technical Publications Glossary PDF and VMware Technical Publications Glossary Online.

Understanding Zones

Horizon Cloud Service with Hosted Infrastructure establishes zones that segregate the different resources based on their function. Horizon Cloud Service has three zones. Each zone is unique to each Horizon Cloud Service deployment and is not shared.

• **Security Zone** – A DMZ where the external Unified Access Gateway appliances reside. It facilitates secure remote access to the Horizon Cloud Service tenant environment.

• **Services Zone** – Where Horizon Cloud Service is hosted, including tenant appliances, utility servers, and internal Unified Access

Gateway appliances.

• **Desktop Zone** – Zone that hosts the desktops and RDSH servers.

Administering the Horizon Cloud Service Environment

You can provision desktops and RDSH desktops and applications through the Horizon Cloud Service Administration Console. You can configure settings for two factor authentication and Active Directory, manage desktop and application entitlements, deploy and update instant and traditional clone images, monitor and observe system and desktop health, and obtain usage and administrative task reports through the web interface.

Managing Desktop and RDSH Server Images

To ensure the best possible user experience, have a properly optimized and configured desktop and RDSH image. With Horizon Cloud Service, you can use your own image or an image provided by the VMware Horizon Cloud Service team. The image is uploaded to the tenant platform. You can complete the installation of applications, tune and optimize the image, make updates, and so on. When your image is ready, it is converted to an image template. You can use this image template for desktop and application assignments in Horizon Cloud Service.

When the image needs to be updated, you can either update an existing image template or upload a new image. To update deployed desktops and RDSH servers, you associate a new image with a desktop or remote application assignment. For more information, see Image Management Strategies.

Connecting to Horizon Cloud Service Desktops and Applications

Horizon Cloud Service users can connect to desktops and applications from a mobile, tablet, thin, or traditional Mac or PC computing device, as well as from a web browser. Users launch the Horizon Client and securely connect to the desktop or application through Unified Access Gateway. The user's connection to the Unified Access Gateway can be through your corporate connection to Horizon Cloud Service or an Internet connection hosted by Horizon Cloud Service. After completing single- or two-factor authentication, you see a list of authorized applications and desktops. Click a resource, and you connect using either the Blast Extreme or PCoIP display protocols.

For devices without Horizon Clients, or if you need quick access to your applications and desktops, you can connect to the Horizon Cloud Service User Portal through the same internal or Internet connection method using a web browser. After you securely log in, you have the option of launching desktops and applications using the VMware HTML5-based client.

Connecting to Corporate or Enterprise Resources

Horizon Cloud Service with Hosted Infrastructure offers several methods of connecting to an existing data center or network with corporate or enterprise applications and data. During the setup process, you can choose from different connection types and speeds, including VPN, Dedicated Connection, MPLS, or Network Exchange. You can also completely isolate your Horizon Cloud Service environment from the corporate network. When users request corporate resources from the virtual desktop or RDSH desktop or application, the network traffic traverses the pre-configured connection between the Horizon Cloud Service data center and your corporate data center.

Some resources, such as user profile or persona, are better served hosted in the Horizon Cloud Service tenant. A utility server, housed in the Services Zone, is a Windows-based server that provides resources for the services supporting the Horizon Cloud Service infrastructure. In addition to user profile and persona data, utility servers can also be configured to deliver Active Directory, VMware User Environment Manager™, DHCP, DNS, and File Services. Some services may require purchasing additional storage.

Figure 2 shows a typical Horizon Cloud Service with Hosted Infrastructure deployment with the network connections between end users, environment, and the Horizon Cloud Service. You can choose whether to allow end users to access their cloud-hosted virtual desktops through the Internet or only when they are on the corporate network.

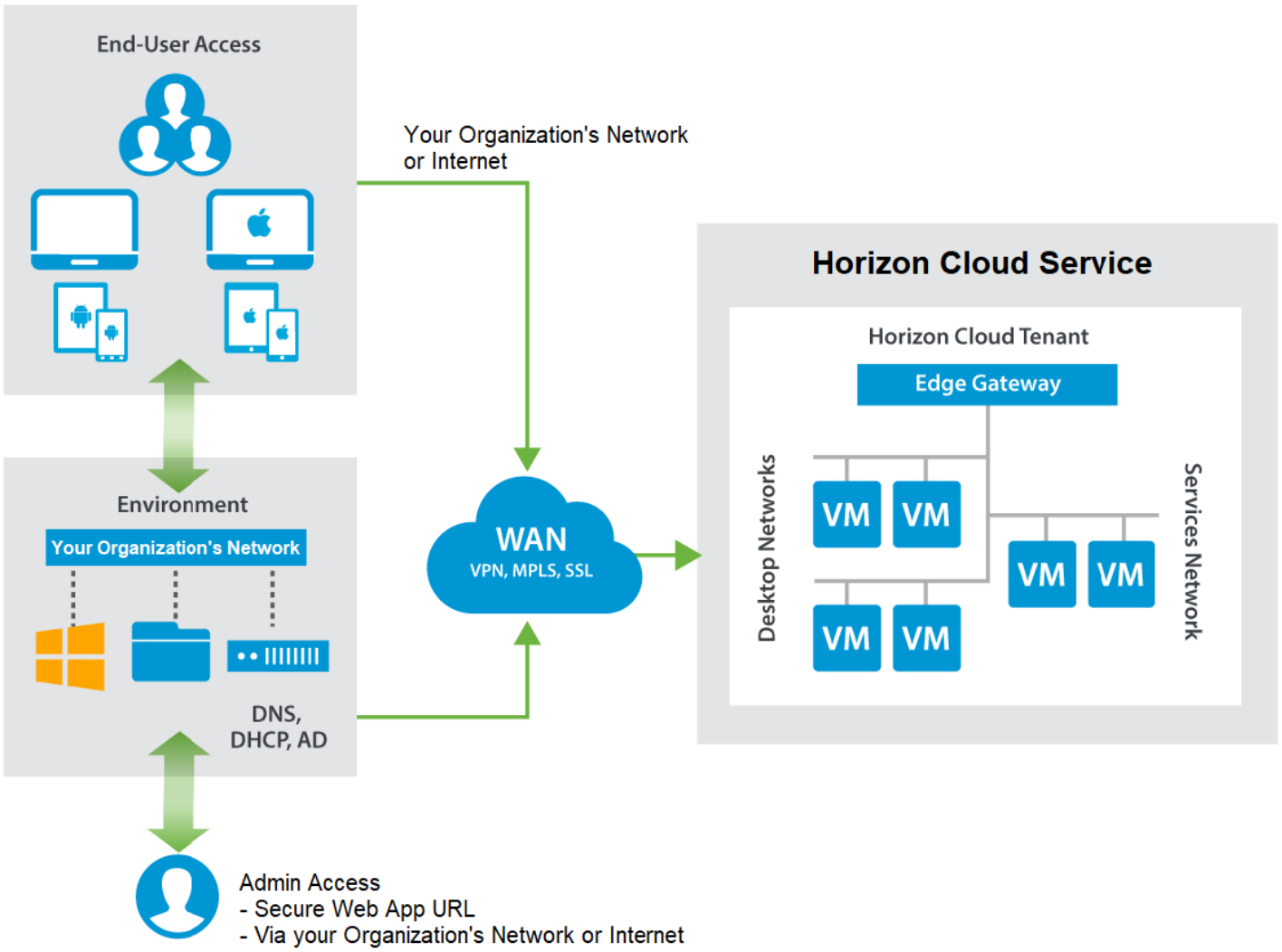

Figure 2: Typical Horizon Cloud Service with Hosted Infrastructure Deployment Model

Integrating User Persona into the Virtual Desktop

You can abstract and manage the user persona with User Environment Manager, which simplifies end-user profile management. User Environment Manager offers personalization and dynamic policy configuration across any virtual, physical, and cloud-based Windows desktop environment. You can configure User Environment Manager to run in the Horizon Cloud Service environment, keeping profiles, persona, and user settings accessible on the utility server.

Avoiding Obstacles That Prolong the Deployment Process

It is a common misconception that you can order hundreds of virtual desktops and simply turn them on with the click of a button. In actuality, it takes time to configure cloud-hosted desktops and connect them to your infrastructure. Preparation of the Horizon Cloud Service environment requires input from your key teams. One of the most effective things you can do to facilitate implementing Horizon Cloud Service is to identify the key stakeholders within your organization and consult with them frequently throughout the planning and implementation phases. You can find the following tips in the navigation bar on the left to help you avoid prolonging the deployment process:

- Establish business drivers, objectives, and project milestones
- Identify key project stakeholders
- Assess desktop need, and identify use cases and user communities

- Gather business and technical requirements data
- Understand the deployment process
- Identify key areas of responsibility
- Complete the Horizon Cloud-Hosted Setup web form
- Discuss platform design considerations
- Attend the kickoff meeting

Establishing Business Drivers, Objectives, and Project Milestones

It is important to understand, quantify, and document why your company is choosing to deliver desktops and applications from a cloud hosting provider. Without understanding why, it is difficult to justify the financial, operational, and business decisions for moving IT services to a cloud-based desktop and application delivery model. Having clear business and technical drivers for adopting Horizon Cloud Service with Hosted Infrastructure is important for gathering business and technical requirements, setting project milestones and objectives, and measuring the benefits.

Several common objectives include:

- **Cloud-first approach** – Many companies have adopted a cloud-first approach instead of on-premises or other data center alternatives because of the operational, financial, and technical benefits, including operational efficiencies and outsourcing tasks associated with hardware and data center management.

- **Simplified IT service delivery** – By implementing a well-defined delivery model to drive an agile and dynamic application and desktop delivery solution, you can accelerate the delivery of IT services to your IT service consumers.

- **Device independence** – When coupled with a secure method of connectivity and identity validation, you can extend access to virtual desktops and applications using untrusted or unmanaged endpoints, removing the costs associated with purchasing laptops for contractors or associates. Supporting various Windows and non-Windows platforms, in addition to thin or zero clients, removes a dependency of connecting to desktops and applications from Windows-only operating systems.

It is also important to establish dates and major project milestones to confirm the availability of resources to complete the necessary tasks for a smooth transition to the cloud. Planning ahead ensures that all aspects of the project are not overlooked during the deployment. The cloud removes responsibility, especially with the hardware platform and some aspects of network connectivity, but some work, such as Active Directory integration and application installation and management, still needs appropriate planning and implementation.

Identifying Key Project Stakeholders

The most common causes for delays in deployment are lack of preparation and communication. Surprises happen when a company subscribes to Horizon Cloud Service without including its security, network, and Active Directory teams in the decision-making process from the beginning. Managing unplanned deployments slows down the process. The better prepared you are, the smoother and faster you can onboard the Horizon Cloud Service platform to your domain.

Identify individuals from the key teams to work with Horizon Cloud Service, including executive sponsorship, line-of-business (LoB) stakeholders, and technical experts, and communicate with them before the deployment process begins to avoid surprises and delays. After setting up the environment, the Horizon Cloud Service team at VMware works closely with your teams to configure and connect to your unique environment. Lack of communication between these key players can result in unexpected problems and slow-downs.

The following key stakeholders provide executive sponsorship and garner support from LoB stakeholders:

ROLE	RESPONSIBILITIES DURING DEPLOYMENT
Project sponsors	Executive sponsor of the project from both IT and executive management
LoB contacts	Sponsor or point of contact from the business units that leverage Horizon Cloud Service with Hosted Infrastructure desktops and applications
Desktop administrators	• Install and configure custom or third-party applications and operating systems on image templates or deployed virtual desktops and RDSH servers • Provide ongoing image management • Create and manage desktop and application assignments • Map assignments to appropriate users within the Active Directory groups • Create desktop and RDSH server images and set them up in the environment • Customize the image templates and perform image updates • Obtain and maintain Windows client OS licensing, if applicable, and compliance with license agreements, if applicable
Server contacts	Provide knowledge of client and server application connectivity and information about servers used for data storage so that they can be routed to and from desktops
Application contacts	• Provide point of contact for major applications that are delivered on cloud-based virtual desktops or RDSH servers • Assist with installation, configuration, and support of major and relevant applications
Networking contacts	• Set up relevant network connectivity to Horizon Cloud Service with Hosted Infrastructure • Decide which DHCP servers and IP subnets and addresses to use • Decide how to configure network access to the Horizon Cloud Service environment • Decide flow and control of inbound and outbound network traffic between your networks and Horizon Cloud Service networks
Active Directory contacts	• Complete Active Directory domain binding • Configure the account used to join RDSH and virtual desktops to the corporate domain • Configure organizational units for virtual desktops and RDSH servers • Configure domain, user- and computer-based group policies, as needed • Define and assign Active Directory users and groups used for desktop and application assignment and tenant administration
Security contacts	• Assist with providing security and compliance requirements • Assist with antivirus and other security-related configurations needed to properly secure the virtual desktops and RDSH servers
Support and operations contacts	Assist with handling support calls and day-to-day IT operations
Project management contacts	• Assist with communication between your teams and the VMware Horizon Cloud Service team • Coordinate resources, deliverables, and project milestones to ensure a successful implementation and deployment

Table 1: Roles and Responsibilities of Key Stakeholders and Subject Matter Experts During Deployment

Conducting Desktop Assessments, and Identifying Use Cases and User Communities

Desktop assessments gather critical application, configuration, and performance information for your current desktop and application environment. This information is used to assess and understand the computing and application usage patterns of your user communities and use cases and is important for determining whether desktop and application virtualization is realistic. This information

is especially important as you move from legacy to newer Windows desktop and application operating systems.

It is recommended that you perform a desktop assessment to help your IT administrators understand the resource demands of your user community. In turn, the assessment helps your IT administrators assign the appropriately sized virtual desktop. For RDSH applications and desktops, this information helps determine the CPU, memory, and disk requirements and the ideal number of concurrent sessions for a single RDSH server. Several industry-proven desktop assessment tools are available to gather desktop and application information. For more information, see SysTrack Desktop Assessment.

In conjunction with desktop assessments, establish which user communities and use cases are good candidates for virtual application and desktop delivery using Horizon Cloud Service with Hosted Infrastructure. Each use case and user community has specific applications, unique business and technical requirements, and different business objectives.

Horizon Cloud Service with Hosted Infrastructure supports multiple use cases, including:

• **Desktop transformation** – Offers the benefits of simplifying desktop management and lowering costs while still providing users with the services they need: access to corporate resources, applications, and data.

• **Remote employees** – Supports geographically dispersed, virtual workers who are telecommuting, offshore, or contracting, and provides access to the corporate environment from their personal devices without concern that sensitive data is at risk of loss or theft because it is not stored locally.

• **Contract and temporary employees** – Supports workers who are not full-time employees and for whom greater security measures and limited access are warranted.

• **Large user groups and communities** – Provides a secure, flexible, and scalable method of delivering and managing virtual applications and desktops to user groups and communities, such as call centers or hospital clinicians, with the same application and desktop platform.

• **Branch offices** – Supports branch offices without requiring local IT departments or infrastructure onsite, and provides connection to a Horizon Cloud Service provider data center that is geographically nearby.

• **Seasonal and cyclical businesses** – Accommodates evolving desktop needs, such as rapid scaling of desktops and applications, and provides desktops for unique tasks or one-off projects, such as environments for building and testing applications.

• **Windows OS migrations** – Extends the life of existing hardware instead of replacing or upgrading desktops to run the latest versions of Windows desktop operating systems, and replaces rich desktops with less costly, more power-efficient thin-client devices.

It is recommended that you tackle lower-risk use cases first, which provide immediate and quantifiable benefits. Tackling the most complex use case first does not necessarily make subsequent use cases easier, because it can result in spending time on troubleshooting that benefits only a small or isolated group of users. Instead, prioritize the use cases based on ease of deployment. Then, solve the use cases according to priority.

Gathering Business and Technical Requirements

Gathering data to meet business and technical requirements helps define which requirements and functionality the platform needs to deliver to your users. Some examples of business and technical requirements include

• **Printing and peripheral support** – The virtual desktop and application solution provides mechanisms to control printing and peripheral device features and functionality. USB device control and printing capabilities can be enforced by polices, Active Directory group policy, and USB device filtering at the endpoint and desktop.

• **Authentication access** – Horizon Cloud Service with Hosted Infrastructure integrates with directory services and two-factor authentication mechanisms for internal and external access. Desktop and application access continues to be handled by mechanisms already in place, such as Active Directory. Single sign-on (SSO) integration is not required.

• **Application integration** – Users must have access to applications on the corporate network.

• **Internet URL and traffic filtering** – Users with desktops in Horizon Cloud Service with Hosted Infrastructure must have all Internet-bound network traffic pass through the corporate URL filtering solution.

If the requirements list becomes extensive or difficult to manage, consider working with a business partner to prioritize which features are absolutely necessary to onboard users onto the platform. You can then add requirements as needed in subsequent releases.

Understanding the Horizon Cloud Service Deployment Process

Deploying Horizon Cloud Service with Hosted Infrastructure can be divided into several basic steps. VMware performs the Capacity Order and Tenant Setup steps, and the remaining steps require the collaboration of your key teams and subject matter experts (SMEs) with VMware.

PROJECT KICKOFF	**Your SMEs with VMware:** • Meet (your lead and VMware lead) • Include desktop manager, desktop engineering, security, and network SMEs in your team • Review and discuss provisioning requirements • Collect information using the Horizon Cloud-Hosted Setup web form • Establish success criteria via VMware-supplied template • Plan next steps			
CAPACITY ORDER	**VMware:** • Orders tenant capacity from data center infrastructure • Configures capacity for Horizon Cloud Service with Hosted Infrastructure			
NETWORK SETUP	**VMware:** • Establishes VPN and VLAN configurations and access • Configures DHCP, DNS, and VPN	**Your SMEs:** • Configure DHCP, Active Directory, and DNS • Provide SSL certificates		
TENANT SETUP	**VMware:** • Sets up Horizon Cloud Service with Hosted infrastructure • Configures storage • Sets up access point • Installs tenant applications • Sets standard desktop capacity			
NETWORK INTERCONNECT	**VMware:** • Installs SSL certificates	**Your SMEs with VMware:** • Test and validate connectivity	**VMware:** • Provides Horizon Cloud Service Administration Console URL • Provides starter image templates	**Your SMEs:** • Perform Active Directory registration • Perform post-test (optional) and install your apps
FINAL SETUP AND TEST	**Your SMEs:** • Install applications into VMware supplied starter image templates	**VMware:** • Imports and moves starter image templates to tenant	**Your SMEs:** • Create images • Create assignments • Assign test desktops and validate	**VMware:** • Conducts knowledge transfer • Establishes support
COMPLETE	**Your SMEs with VMware:** • Agree that setup is complete • VMware provides advanced onboarding services (optional) • Verify that all success criteria are met			

Table 2: Overview of the Horizon Cloud Service with Hosted Infrastructure Deployment Process

Internal processes, such as onboarding and help desk procedures, can change when you adopt a virtual desktop environment. Before deploying a virtual desktop environment, make sure that you understand the differences between a standard desktop environment and a virtual one. Operational readiness helps ensure a successful deployment.

The entire deployment process depends on your environment and requirements. The two most effective ways to expedite this process are to prepare for the kickoff meeting and to facilitate communication within your company.

Identifying Key Areas of Responsibility

A successful and expedient deployment depends on good communication between the teams impacted by Horizon Cloud Service so that they work together in a well-integrated manner before, during, and after the kickoff. Make sure that a representative from each team does the following:

• Reviews the Horizon Cloud-Hosted Setup web form early to be able to ask questions or voice concerns before the kickoff meeting.

• Discusses and documents company-specific platform design considerations or requirements, including directory services, printing and peripherals, remote access and authentication, user environment and application data management, operations and support, and image management.

• Attends the kickoff meeting so that all representatives receive the same initial instructions and training. At the meeting, participants also have a chance to ask questions, voice concerns, and resolve problems.

Figure 3 shows the areas of ownership in a typical Horizon Cloud Service with Hosted Infrastructure deployment. The Meet Me Room represents the point of demarcation where the outside connections come into the data center, such as an outside dedicated connection, MPLS line, or network exchange connecting with the Horizon Cloud Service network.

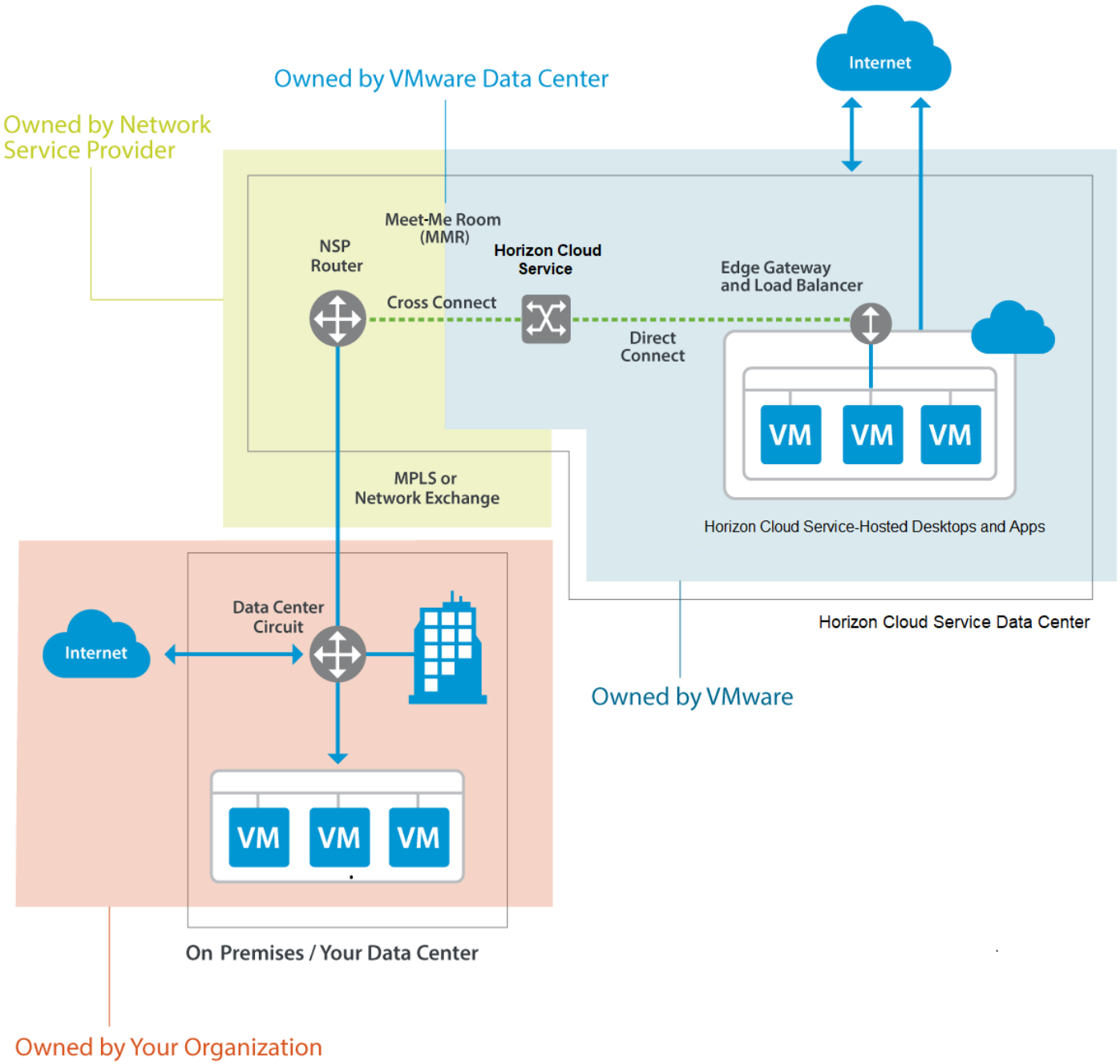

Figure 3: Example Areas of Ownership

Your key stakeholders and SMEs are primarily responsible for

- Providing corporate resource assistance for establishing and maintaining site-to-site connectivity
- Completing Active Directory domain binding and creating necessary domain join and service accounts
- Building and customizing your image templates
- Creating desktop and application assignments and assigning them to end users
- Packaging applications for dynamic application delivery using VMware ThinApp®, or other application packaging technology
- Installing and configuring endpoints with the Horizon Client (if applicable)

• Providing Windows Client OS and application licensing (if applicable, and if so, compliance with all necessary license agreements)

• Installing and configuring applications, patches, security fixes, and other relevant software and operating system updates on image templates or deployed desktops and RDSH servers

• Creating new desktop and application assignments or deploying new and updated images and applications to existing desktop pools or RDSH servers

The VMware Horizon Cloud Service team is responsible for:

• Implementing service hardware components (physical servers, physical storage, and physical network devices) needed to support contracted virtual resource pools

• Providing initial network resources, including a default public IP address

• Providing standard desktop capacity, which includes memory, processing, primary storage, and networking

• Enabling a secure point-to-point network interconnect (also known as the backhaul connection) via VPN, MPLS, or Network Exchange from the Horizon Cloud Service network to your corporate network

• Providing 10 standard VMware-approved images from the image catalog

• Providing 2 hours of live demo of the Horizon Cloud Service Administration Console

• Providing access to self-service training videos

Designate individuals who are authorized to access Horizon Cloud Service with Hosted Infrastructure online support portals. These contacts are authorized to make service requests, open support tickets, and receive maintenance notifications.

Completing the Horizon Cloud-Hosted Setup Web Form

The Horizon Cloud-Hosted Setup web form helps you prepare for the deployment process by identifying the individuals involved during and after deployment. After you subscribe to Horizon Cloud Service, VMware emails you a link to the form. To log in to the web form, you need a valid `my.vmware` account. Gathering this information before the process begins can save time by preventing delays during implementation. You can find an example in the Horizon Cloud-Hosted Setup Guide, which is provided to you before the kickoff meeting. Make sure that the representative from each key team reviews the Horizon CloudHosted Setup web form early to ask questions or voice concerns before the kickoff.

Discussing Platform Design Considerations

It is important to understand the requirements and design considerations that are unique to your environment. The Horizon Cloud Service platform is standards-driven, scalable, and secure, but every company deployment has unique characteristics, including varying business and technical requirements, use cases and user communities, applications, desktop settings and configurations, and feature and functionality requirements.

Review the topics in Table 3 to ensure that all elements of a virtual desktop and application delivery solution are covered. Each topic can involve one or more of the key stakeholders for the project, who should interact with their peers to reach sensible, achievable, and realistic design decisions that meet business needs and demands.

TOPIC	DESCRIPTION
Endpoints and user communities	Use cases, end-user communities, and endpoints that access Horizon Cloud Service with Hosted Infrastructure virtual desktops.
Printing and peripherals	Printing requirements, infrastructure, and peripheral devices used in the enterprise and the proposed approach and design considerations for printing and peripheral device integration in the virtual desktop environment.
Desktop and application pool standards	Horizon Cloud Service with Hosted Infrastructure critical design elements, including desktop pool standards, tenant-specific configurations, and desktop communication protocols.
Directory services and group policies	Active Directory implementation and integration considerations for the Horizon Cloud Service with Hosted Infrastructure environment.
Access and authentication	Methodology, mechanisms, and requirements for accessing and authenticating to the Horizon Cloud Service with Hosted Infrastructure environment.
Backup, recovery, and business continuity	Backup and recovery processes for Horizon Cloud Service with Hosted Infrastructure applications, desktops, and user data. Alternative methods for expanding capacity for business continuity events or methods to recover virtual desktop and application services in an alternative location.
Desktop security	Desktop security requirements and antivirus and endpoint-protection strategies.
Application integration	Desktop, virtual machine, and Horizon Cloud Service with Hosted Infrastructure considerations as they relate to virtual and physical application integration.
Application data and persona management	Application setting persistency and user persona and profile standards when using Horizon Cloud Service with Hosted Infrastructure virtual desktops. Evaluates the location of data in relation to the virtualized desktop.
Support and operations	Support process for tenant administrators and IT users, operational policies and procedures for managing applications, desktop and RDSH images, patch management, software deployment, and so on.
Multimedia and unified communications	Multimedia and unified communications requirements and configurations for the project, including real-time audio-video (RTAV) and graphics acceleration.

Table 3: Platform Design Considerations

In addition to addressing tenant-specific design considerations, all teams should gather the information needed to complete the Horizon Cloud-Hosted Setup web form. Lack of preparation is one of the most common causes of delays.

Attending the Kickoff Meeting

At the kickoff meeting, you can explain the deployment process, timeline, and requirements. Make sure that representatives from all key teams attend the kickoff meeting to clarify who is responsible for what and where to go if questions or problems arise. The kickoff meeting demystifies the deployment process and provides an opportunity for consensus building at the start of the process. See Identifying Key Areas of Responsibility.

Choosing Strategic Network Options

Consult your network team about the requirements and types of network connections needed to operate successfully with Horizon Cloud Service. Involving representatives from your networking team early minimizes possible delays during the initial deployment because much of the implementation relies on networking. It also allows them to ask questions, voice concerns, and address issues early on. It is important to engage the necessary management and networking personnel with the appropriate skill sets to address the following considerations and efficiently facilitate the integration of VMware Horizon Cloud Service with your environment. You can find the following considerations in the navigation bar on the left:

- IPsec VPN, dedicated connections, MPLS, and Network Exchange options
- Choosing the ideal network connection
- Horizon Cloud network options
- Firewall exceptions and required ports
- Unified Access Gateway
- Network routing
- IPsec VPN parameters (optional)

IPsec VPN, Dedicated Connections, MPLS, and Network Exchange Options

Determining the type of network connection to implement is an important step before deploying Horizon Cloud Service. The network connection delivers Horizon Cloud Service desktops and RDSH server access to applications and data in your data center and network. It also provides a path for users, both inside and outside the network, to connect to Horizon Cloud Service desktop and application resources. You can use one or more of the following methods to connect users to desktops, data, and applications (see the navigation bar on the left):

- Accessing Horizon Cloud with Hosted Infrastructure desktops and applications from the Internet
- Sending traffic through a site-to-site IPsec VPN
- Sending traffic through a dedicated connection or MPLS Direct Connect VPN
- Sending traffic through a network exchange
- Connecting your existing rack if in the same data center
- Reducing traffic over the back haul

Figure 4 shows access options using IPsec VPN, dedicated connection, MPLS, Network Exchange, or your rack.

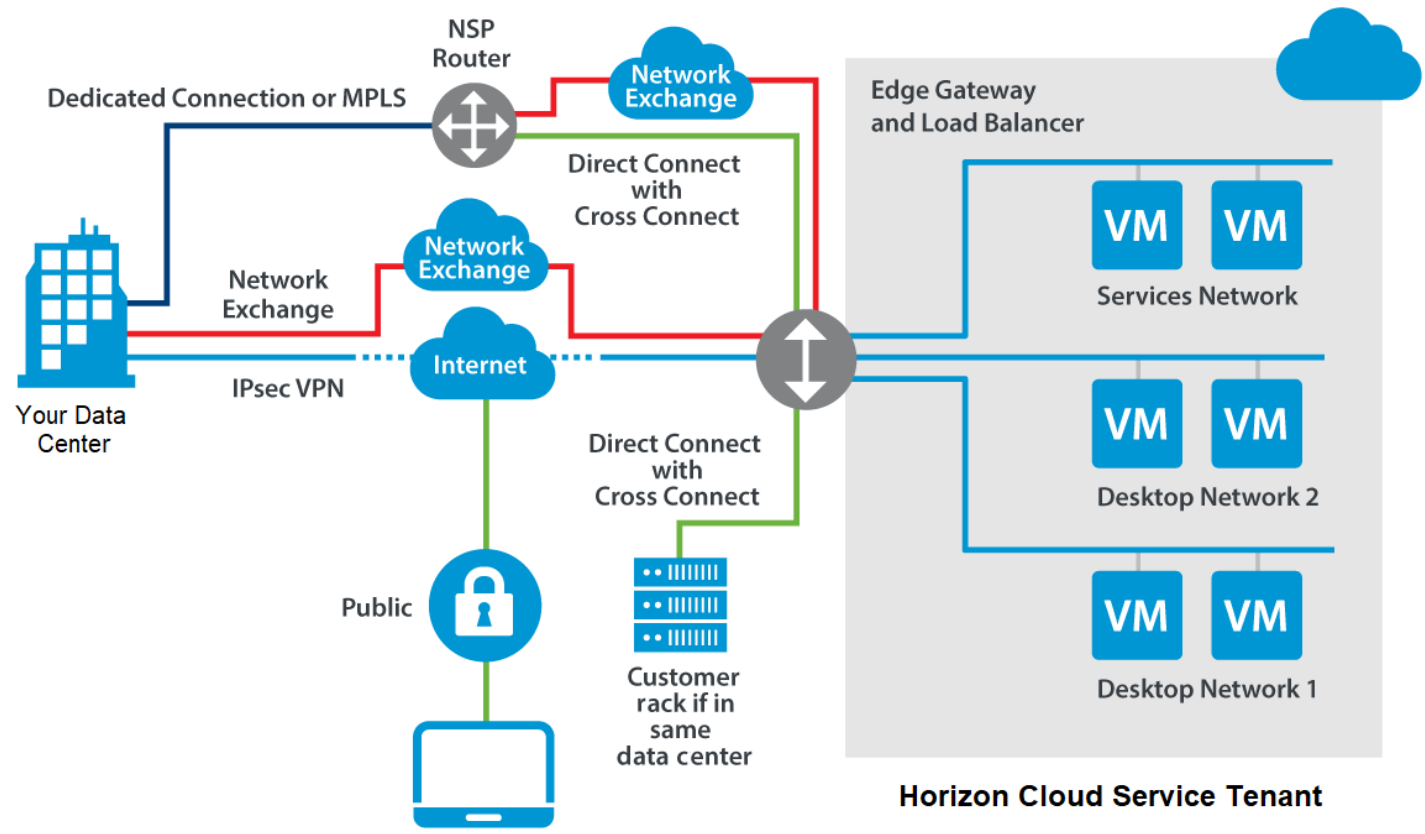

Figure 4: Access Strategy Methods for a Horizon Cloud Service with Hosted Infrastructure Deployment

Accessing Horizon Cloud Service with Hosted Infrastructure Desktops and Applications from the Internet

Horizon Cloud Service supports direct Internet access to Horizon Cloud Service with Hosted Infrastructure desktops and applications without passing through your corporate infrastructure first. This type of connection is particularly convenient for users working from home or another remote location. The connection can be secured with RSA SecurID or RADIUS-compliant two-factor authentication solutions. Internet-based connections are part of the standard Horizon Cloud Service offering. An alternative connection (VPN, MPLS, or Network Exchange) is required to access Horizon Cloud Service resources from inside your network.

Sending Traffic Through a Site-to-Site IPsec VPN

Site-to-site (S2S) IPsec VPNs connect separate networks to each other through the public Internet. For example, a branch office network can connect by site-to-site VPN to a headquarters network. Each site on the network is equipped with a VPN gateway, such as a router, firewall, VPN concentrator, or security appliance. For more information, see Types of VPN Access.

Building an S2S IPsec VPN tunnel is relatively simple and inexpensive, but it is subject to interruptions that can affect latency. Latency is any type of delay experienced while processing network data. Because the VPN tunnel is built through the public Internet, congestion, connection types (satellite, ADSL, and others), or other network-related problems can occur on the Internet that cause latency to spike. Latency spikes caused by the public Internet are beyond the control of you or Horizon Cloud Service.

The S2S IPsec VPN tunnel includes logical and encrypted point-to-point connections between Horizon Cloud Service instances and your corporate site, providing secure access to your corporate data center services, such as business applications, Active Directory, DNS, and DHCP servers. It also provides a secure connection for protocol traffic originating from your corporate networks.

Parameters, such as the Security Association (SA) lifetime timers, which define the lifetime that a given tunnel uses to encrypt data, are not changeable in the Edge Gateway and therefore must be changed on your equipment to match those on the Horizon Cloud Service side. Both Phase 1 and Phase 2 of the deployment include SA lifetime timers. When the timer expires, it renegotiates authentication for both sides. If the SA lifetime timers are not set on the tenant side to match the Horizon Cloud Service side, they can cause problems in the VPN tunnel. For more information, see IPsec VPN Parameters.

Sending Traffic Through a Dedicated Connection or MPLS Direct Connect VPN

A dedicated connection or MPLS routes traffic within a telecommunications network as data travels from one network node to the next. Building an MPLS Direct Connect VPN tunnel has a higher cost than creating an S2S IPsec VPN connection, but MPLS Direct Connect is free of the interruptions that can occur on the public Internet. Latency is typically guaranteed by the Direct Connect provider. The cost of the service depends on the options you choose and the amount of dedicated bandwidth you require.

Sending Traffic Through a Network Exchange

A network exchange, or what is also commonly known as a cloud exchange, is a service that connects your private network using your preferred network service provider with cloud service providers, such as Horizon Cloud Service, using secure, high-throughput, low-latency connections.

Using a network exchange usually has a lower cost than creating a MPLS Direct Connect VPN tunnel and, in most cases, can be activated within hours, reducing the overall time it takes to connect Horizon Cloud Service to your corporate site. Horizon Cloud Service offers Equinix Cloud Exchange as the network exchange option.

Connecting Your Existing Rack If in the Same Data Center

If you already have IT resources and services that are collocated in the same data center as Horizon Cloud Service, you can connect your existing environment to your Horizon Cloud Service tenant. To achieve this, a Direct Connect with Cross Connect is required between your rack and Horizon Cloud Service.

Reducing Traffic over the Back Haul

You can leverage the Horizon Cloud Service–provided Internet connectivity to access desktops while saving the back-haul dedicated connection, MPLS, VPN, or Network Exchange data for internal desktop users and tenant application and data-related network traffic. This approach saves the back haul for critical network traffic while leveraging the bandwidth of the VMware Internet connection.

For more information, see the Horizon Cloud-Hosted Setup web form.

Choosing the Ideal Type of Network Connection

Consult the Horizon Cloud Service team when choosing a routing option. The choice depends on a number of variables within your environment, including the amount and type of desktops and the type of traffic, as follows:

• **Desktops** – IPsec VPN is generally best for fewer than 500 desktops. A dedicated connection, MPLS Direct Connect, or Network Exchange is usually best for more than 500 desktops. A growing organization should consider switching to a dedicated connection, MPLS Direct Connect, or Network Exchange when over 500 desktops.

• **Traffic** – If your desktops are used for minimal actions such as email, you can probably use IPsec VPN until you have more than 500 desktops. If all end users are accessing the platform simultaneously or making large FTP transfers, consider a dedicated connection, MPLS Direct Connect, or Network Exchange at 500 desktops.

If you experience performance problems with an S2S IPsec VPN, the solution is beyond the control of your organization or VMware support. When you use a dedicated connection, MPLS Direct Connect, or Network Exchange, the circuit is yours from end to end, and you can call the provider to resolve any issues.

Horizon Cloud Service Network Options

If you are using a dedicated connection, MPLS, Network Exchange, or your own rack in the same data center, you have several options to extend your data center and services into Horizon Cloud Service. Horizon Cloud Service offers a Direct Connect with Cross Connect 1 GB or 10 GB, along with a Direct Connect with Network Exchange 1 GB or 10 GB.

Considering Protocol, In-Guest, and Internet-Bound Traffic

Understanding traffic flows associated with Horizon Cloud Service is key when choosing the type of network to implement, and it is an important step before deploying Horizon Cloud Service. You need to consider protocol traffic generated by Horizon Clients and network traffic generated by applications and other services on Horizon Cloud Service desktops and RDSH servers.

Note: At a minimum, S2S VPN, Dedicated Connection, MPLS, or Network Exchange is needed for AD, DNS, DHCP, and NTP, except in island accounts. An island account has no connectivity to the tenant site, so all access into the system is from the public Internet. An island account is usually used only for pilot implementations in which Horizon Cloud Service hosts basic Active Directory, DNS, DHCP, and NTP services and configurations.

Protocol Traffic

Protocol traffic is created when a user connects to the Horizon Cloud Service environment. The flow of protocol traffic starts when the user moves the mouse or types on the keyboard. Users connect to Unified Access Gateway, the secure gateway that tunnels them into the tenant appliance. Users are presented with desktops and applications through the traditional Horizon Client or the Horizon Cloud Service User Portal. Users can select the desktop or application they want to launch. Depending on the client used to connect there are two protocol choices: Blast Extreme or PCoIP.

For more information, see Technical Introduction to Access Point for Secure Remote Access.

Blast Extreme

Blast Extreme is the recommended protocol for a Horizon Cloud Service implementation because it adapts to network conditions to provide an optimized desktop delivery across both a LAN and a WAN. Out of the box, Blast Extreme works well for most workloads. Using a Group Policy Object (GPO)—a collection of settings that define how a system behaves for a specific set of users—you can optimize your end-user experience.

Blast Extreme optimization settings are configured in the agent using the `vdm_blast.adm` group policy template. Some of the settings involve:

• **Bandwidth and frame rate** – You can use Blast Extreme to display images remotely. Image transmission is compressed to reduce the amount of bandwidth used. Based on the use case, you can modify the frame rate or the number of individual images transmitted per second to reduce the amount of bandwidth.

• **Whether to use UDP transport** – Blast Extreme can leverage both TCP and UDP to transmit packets of data over the Internet. UDP is typically used when speed is the most important consideration, such as live broadcasts or online games.

• **Whether to use the H.264 codec** – By default, Blast Extreme uses the H.264 codec. But in some use cases, specifically where lossless image display is necessary, you can use the JPG or PNG codec.

• **Image quality for the JPG, PNG, and H.264 codecs** – You can reduce the image-quality components to reduce bandwidth consumption for specific use cases.

For more information, see Blast Extreme Display Protocol in Horizon 7 and VMware Blast Policy Settings in Setting Up Desktop and Application Pools in View. For instructions on importing the template, see Add View ADM Templates to a GPO in Setting Up Desktop and Application Pools in View.

PCoIP

PCoIP is an alternative protocol for accessing Horizon Cloud Service with Hosted Infrastructure desktops and applications. You can use PCoIP with traditional Horizon Clients and Teradici zero clients for access to Horizon Cloud Service.

PCoIP optimization settings are configured in the agent using the `pcoip.adm` group policy template. Some of the settings are:

• **Max link rate** – Sets the maximum session bandwidth. The default is 1 Gbps.

• **Minimum image quality** – A higher number shows a crisper image but choppier motion. A lower number has smoother motion but a less crisp image. The default is 40 percent of fully lossless.

• **Maximum initial image quality** – A higher number shows a better initial image, but requires more bandwidth for screen changes. A lower number provides a lower-quality initial image, but requires less bandwidth for screen changes. The default is 80 percent of fully lossless.

• **Turn off build-to-lossless feature** – Do not enable this setting if you need high-quality images. For example, medical imaging needs build to lossless because it provides the highest-quality images. The default is enabled, which means that images are not built to lossless. • Configure the PCoIP session audio bandwidth limit – Sets the usable audio quality setting. The default is 500 kbps.

• **Maximum frame rate** – A higher number uses more bandwidth, but creates smoother motion in an image. A lower number uses less bandwidth, but provides choppier motion in an image. The default is 30 frames per second (fps).

For more information, see Horizon 6 with PCoIP—Up to 30% Bandwidth Savings out of the Box, VMware Horizon 6 with View Performance and Best Practices, and VMware View 5 with PCoIP.

In-Guest Traffic

In-guest traffic is created when an application makes a network call to another application or IT service from within the desktop. An example is when the browser launches from the desktop and reaches out to an internally hosted corporate website. In-guest traffic includes any action within the desktop, except for Internet-bound network traffic and when the user moves the mouse to launch the browser, which is considered protocol traffic.

By default, all in-guest traffic is routed over the corporate VPN, Dedicated Connection, MPLS, or Network Exchange connection. Routing all traffic over these links can create traffic jams, so establish alternative routes indicating which network IP address and subnets to connect to. The Horizon CloudHosted Setup web form lists the data required to create alternate routes, including specifying your core servers, such as Active Directory, DNS, DHCP, NTP, FTP, and file servers.

Routing Internet-Bound Traffic

A key step in the process is choosing how Internet traffic is routed from Horizon Cloud Service desktops and applications, such as via an Internet connection provided by Horizon Cloud Service or through your own network. How Internet traffic is routed within the VMware data center varies depending on which routing option you choose for the default route (0.0.0.0/0).

In the following scenarios, a user tries to access an Internet website from a virtual desktop within Horizon Cloud Service. The desktop sends the request to the corresponding Edge Gateway. In each scenario, the Edge Gateway responds differently depending on the routing option:

• **Option 1 – Internet Traffic routed out of the Horizon Cloud Service Internet Connection** – The Edge Gateway sends the request to the Internet, using the default route with Network Address Translation (NAT) via the VMware-provided Internet connection. From there, the request traverses the Internet like any other packet until it reaches its destination. This traffic is unfiltered.

• **Option 2 – Internet Traffic routed across an IPsec VPN** – The Edge Gateway encapsulates the request into an IPsec tunnel and sends it to the user's corporate site via the default route. The corporate site receives the request and can then drop the request if the website is considered inappropriate or route the request to the corporate network and out to the Internet.

• **Option 3 – Internet Traffic routed across Dedicated Connection, MPLS Direct Connect, or Network Exchange** – The Edge Gateway sends the request to the corporate Dedicated Connection, MPLS Direct Connect, or Network Exchange via the default route on the Edge Gateway. The corporate site receives the request and can then drop the request if the website is considered inappropriate or route the request to the corporate network and out to the Internet. However, this method has a limitation. If the default route points down the Dedicated Connection, MPLS Direct Connect, or Network Exchange, external access into the environment is technically not possible. You can also choose not to use the VMware-provided Internet connection and have all user connections over the WAN link but seen as internal connections due the nature of the connection not originating externally.

For security reasons, many companies are concerned about inappropriate web traffic and want their Internet traffic to route over their VPNs, Dedicated Connection, MPLS, or Network Exchange when the traffic returns to the corporate site. This process allows them to monitor and filter the traffic and prevents visits to illicit sites. This option is not recommended when using Dedicated Connection, MPLS Direct Connect, or Network Exchange, because it can break the protocol traffic coming in from the Internet, preventing users from connecting remotely to the environment (Option 3).

Instead, the following secure options for routing in-guest traffic through the VMware data center are supported:

• **Proxy server** – The Edge Gateway is configured for Option 1, but your desktop Internet traffic connects to your corporate site through a proxy server located in your corporate data center or office. With the default route configured to use the VMware-provided Internet link of the Edge Gateway, and the desktops configured to send all Internet traffic back to the proxy server, your site is protected from risks related to web traffic by an IDS, IPS, or firewall, and remote users are still able to connect to their Horizon Cloud Service desktops and applications from the public Internet. This option creates more work for you because you must run the proxy server from your corporate data center, but it is the best of both Option 1 and Option 3.

• **Third-party cloud-based DNS** – You can use a third-party cloud-based DNS service, that includes phishing protection and content filtering, to limit what users can do while logged in. For example, if an end user tries to go to an inappropriate site, the DNS server does not respond.

Firewall Exceptions and Required Ports

Your networking team collaborates with the VMware Horizon Cloud Service team to set up firewall exceptions. Open firewall ports include all remote connections going to or from the endpoint device, tenant appliance, and Unified Access Gateway. Your users communicate with Horizon Cloud Service through LDAP, AD, DNS, DHCP, and NTP ports, as well as ports to FTP, SSH, file servers, and so on. Table 4 describes the ports used with Horizon Cloud Service. Check with your Horizon Cloud Service representative to

verify that this information is accurate for your site.

SOURCE	DESTINATION	PORTS IN USE	DESCRIPTION
Horizon Cloud Service	Your Active Directory infrastructure	TCP/389 UDP/389	Authenticates users to the Horizon Client, VMware Horizon Cloud Service User Portal, and the Horizon Cloud Service Administration Console using LDAP or LDAP SASL GSSAPI for secure authentication. The configured user groups and their members are cached in the tenant fabric for performance purposes.
Horizon Cloud Service	Your Active Directory infrastructure	TCP/3268	Performs Active Directory Global Catalog lookup and searches.
Horizon Cloud Service	Your Active Directory infrastructure	TCP/88 UDP/88	Used for Kerberos authentication.
Horizon Cloud Service	Your DNS	TCP/53 UDP/53	Used for DNS.
Horizon Cloud Service	RSA Authentication Manager	UDP/5500	Communicates with RSA Authentication Manager when SecurID is in use by the tenant. The Authentication Manager can be located in a different data center from the tenant appliances. A high-availability authentication manager used for failover can also be located remotely.
Horizon Cloud Service	Your RADIUS server	UDP/1812 UDP/1813	Communicates with RADIUS-based authentication when RADIUS is in use by the tenant.
Your site or endpoint device	Horizon Cloud Service	TCP/8443 UDP/8443	Used for Blast Extreme.
Your site or endpoint device	Horizon Cloud Service	TCP/443 UDP/443	Used for Blast Extreme.
Your site or endpoint device	Horizon Cloud Service	TCP/4172 UDP/4172	Used for PCoIP.
Your site or endpoint device	Horizon Cloud Service	TCP/80, TCP/443	Access to the VMware Horizon Cloud Service User Portal and the Horizon Cloud Service Administration Console. Also used by the native Horizon Client to initially connect to Horizon Cloud Service resources. If remote access is enabled, the User Portal must be made publicly available. Port 80 redirects to port 443.

Table 4: Horizon Cloud Service Ports

Unified Access Gateway

VMware Unified Access Gateway (formerly Access Point) is a hardened Linux virtual appliance that allows secure remote access into the Horizon Cloud Service environment. If your workers use an external connection via the public Internet—whether the traffic is web-based or protocol-based—the traffic is sent to Unified Access Gateway. Unified Access Gateway acts as a secure proxy for your connection into the Horizon Cloud Service environment. The Unified Access Gateway proxies Horizon Cloud Service traffic to and from the Security Zone. The Security Zone is a demilitarized zone (DMZ) networking security construct that gives a segment of the corporate network access to the outside but with strict rules regulating access to what is inside your network.

Network Routing

Horizon Cloud Service supports both static routing and dynamic routing, allowing traffic to properly pass between Horizon Cloud Service and your internal network segments. Dynamic routing capabilities for Dedicated Connection, MPLS Direct Connect, or Network Exchange-based connections are offered using BGP, a standardized exterior gateway protocol for exchanging routing information between systems on the Internet. Dynamic routing via External BGP (eBGP), a BGP extension used for communication between autonomous systems, allows routing changes to be automatically propagated to Horizon Cloud Service. When eBGP is used with the proper path attributes, you can select which redundant link is active. It also ensures that automatic failover between multiple MPLS connections is supported. You are responsible for assigning the BGP autonomous system number to the Horizon Cloud Service router, which is usually a private number in the 65xxx range. Static routing is available if you cannot support BGP routing.

For VPN-based connections to Horizon Cloud Service, static routing is configured during the VPN peering process. If other networking routing questions arise, notify the Horizon Cloud Service team as soon as possible so that they can be addressed.

IPsec VPN Parameters (Optional)

The Horizon Cloud-Hosted Setup web form lists the required and optional IPsec VPN protocols and parameters if you choose to set up an S2S VPN between your network and the VMware data center. For IPsec VPNs, Horizon Cloud Service uses Edge Gateway, a virtual appliance that provides additional security options and features, such as dynamic routing via Border Gateway Protocol (BGP). Edge Gateway supports Main mode for Phase 1 and Quick mode for Phase 2. For clarification on these terms, consult your networking engineer or the VMware NSX 6 Administration Guide.

Table 5 lists the protocols and parameters to use in each phase. You must set the same protocols and parameters for each phase on your network as are set in Horizon Cloud Service. For example, ISAKMP parameters are used for Phase 1, IKE parameters are used for Phase 2, and Oakley protocols are used for authentication, as well as MODP Group 2. Currently, all parameters are required. In the upgrade to Edge Gateway, the Phase 2 Perfect Forward Secrecy (PFS) for rekeying is optional.

PROTOCOLS AND PARAMETERS	PHASE 1	PHASE 2
Hash (SHA or MD5)	SHA1	SHA1
Authentication mode	Main	Main
Encryption	AES256	AES256
Diffie-Hellman Group (1, 2, or 5)	2	2
Encapsulation (AH or ESP)	N/A	ESP
Lifetime	28800	3600
Perfect Forward Secrecy	N/A	True. Requirements of shared secret: You can provide your own shared secret, or Horizon Cloud Service can generate a random shared secret to use on both sides. • Between 32 and 128 characters • At least 1 uppercase letter • At least 1 lowercase letter • At least 1 number • No special characters

Table 5: Recommended IPsec VPN Configuration

Note: Some parameters, such as the Security Association lifetime timers, cannot be changed in Edge Gateway and must be changed on the tenant equipment to match those in Edge Gateway. When the SA timer expires, it renegotiates authentication for both sides. Edge Gateway does not re-authenticate on traffic, only on the lifetime timer. If the timer settings on Horizon Cloud Service and on the tenant side do not match, the VPN tunnel can bounce.

Meeting Active Directory Requirements

It is important to set up your AD before deploying Horizon Cloud Service. Consult your AD team early and often throughout the deployment process. Include representatives from your Active Directory team with proper Domain Admin permissions in the decision-making and deployment process, from the start. This enables everyone to ask questions, voice concerns, and address any issues early in the deployment. Topics to consider include (see the navigation bar on the left):

• Choosing an existing or isolated AD

• Creating service accounts for AD

• Creating groups for AD

• Creating a unique Horizon Cloud OU for AD

• Setting up DHCP scopes and Option Code 74 or manually configuring DaaS agents

Choosing an Existing or Isolated Active Directory

Although the Horizon Cloud Service platform relies on AD, you are not required to integrate Horizon Cloud Service with an existing AD environment. You can use a separate, isolated AD domain that is local to the Horizon Cloud Service desktops and applications service. You can request an isolated domain from the Horizon Cloud Service team. Choosing a pilot domain is advantageous for the following use cases:

• **Companies with outsourced users** – If your company offloads development work to other countries, you need to provide employees with desktops, but you might not want them connecting directly into your own infrastructure. In a pilot domain, you can set up everything those employees need in an isolated environment.

• **Companies with seasonal users** – If your company has seasonal work that ramps up two or three times a year for a couple of months, you might not want to add a large number of desktops to your corporate AD structure. You can use a separate pilot domain when you need it and discard it when the season is over.

• **Companies with limited resources** – If your company has limited infrastructure, you can use a separate isolated domain to save the cost of building a primary directory services infrastructure.

Creating Service Accounts for Active Directory

Two types of service accounts are required if you choose to integrate the Horizon Cloud Service environment with an existing Active Directory: domain bind and domain join. The domain bind account parses through your AD structure and pulls in all users designated for Horizon Cloud Service. The domain join account joins the virtual desktops and RDSH servers to the AD domain. For more information, see *Register Your First Active Directory Domain* in Horizon Cloud with Hosted Infrastructure Administration.

See the Horizon Cloud-Hosted Setup web form for examples.

Creating Groups for Active Directory

To effectively map users to desktops, applications, and tenant administration functions within the Horizon Cloud Service platform, it is prudent to create groups in AD for each type of role, function, and access. Keep the following points in mind to maintain compatibility with the Horizon Cloud Service platform:

• **Avoid nesting** – Do not create nested groups to ensure efficient AD object lookups. User objects are the only members of a group.

• **Avoid mixing** – Do not mix members from multiple domains (child or trusted) in the same group.

• **Create groups** – Create separate groups for tenant administration, help desk support, testing and validation users, and production users. If multiple domains are configured for a Horizon Cloud Service tenant, IT administrators should create similar groups for tenant administration, help desk support, testing and validation users, and production users for each individual domain. Tenant administrators

have access to the Horizon Cloud Service Administration Console. Testing, validation, and production user groups are used to provision access to Horizon Cloud Service desktops and applications.

Creating a Unique Horizon Cloud Service OU for Active Directory

A large company with thousands of OUs and groups can easily have hundreds of thousands of objects in its AD. The company could save deployment time by implementing a unique OU for computer accounts that are created by the Horizon Cloud Service platform. The unique OU avoids the need for Horizon Cloud Service to parse the entire AD for virtual desktop and RDSH server computer objects.

See the Horizon Cloud-Hosted Setup web form for a list of users, accounts, and permissions needed.

Setting Up DHCP Scopes and Option Code 74 or Manually Configuring DaaS Agents

You must provide the VMware Horizon Cloud Service team with a services subnet and a desktop subnet that are not being used inside your infrastructure, and those subnets must include enough IP addresses to cover the number of desktops or RDSH servers that are provisioned. Setting Option Code 74 in the desktop subnet DHCP scope directs the desktops and RDSH servers to the tenant appliances. The VMware Horizon Cloud Service team provides the two IP addresses of the tenant appliances during the deployment process.

Watch out for the following issues:

• **Failure to set Option Code 74 properly** – If not done properly, the desktops and RDSH servers are unable to locate and register with the tenant appliances. End users are unable to access published desktop and application resources.

• **Failure to provide a unique services and desktop subnet** – Think of the services and desktop subnet as an extension of your local infrastructure, even though it is in the cloud. If you provide a subnet that is already in use, conflicts can occur, and network traffic might not properly flow between Horizon Cloud Service and your network.

• **Failure to consider sizing** – If you do not provide a desktop subnet with enough IP addresses to cover the targeted number of desktops and RDSH servers, you must set up another subnet to support the increased capacity. For example, if you provide the /24 in CIDR format for the subnet, you get exactly 252 addresses. Adding additional subnets upfront allows for seamless capacity expansion when needed.

If you cannot configure DHCP Option 74 due to network constraints or other reasons, you can manually configure the DaaS Agent to communicate to the tenant appliances. The VMware Horizon Cloud Service team provides the two IP addresses of the tenant appliances and manually configures the DaaS Agent using the `monitor.ini` file.

Creating Optimized Images

Image optimization ensures that the virtual desktop or RDSH server is properly configured to provide an optimal end-user experience. You can adjust optimization settings statically or dynamically based on your needs and network requirements and conditions. An unoptimized image can consume unnecessary compute, network, and storage resources, potentially contributing to a substandard end-user experience.

It is important to create optimized images before deploying Horizon Cloud Service and to consult your desktop image management team early and often on the following issues, which you can find in the navigation bar on the left:

• Optimizing desktop images

• Deciding how many images you need

• Using traditional or instant clone images

• Creating images for RDSH servers

• Understanding dedicated, floating, and session desktops

• Choosing 3D graphics options

• Staggering automatic antivirus updates

Optimizing Your Desktop Images

An image template, sometimes called a master image or gold pattern, is the standard base desktop or RDSH server image provided by Horizon Cloud Service. An image template is fully optimized with all the VMware tools and Horizon Cloud Service desktop service agents that are required for the platform. It is recommended that you install your software packages on the optimized image templates to take advantage of the tools and service agents that are preinstalled and configured in accordance with VMware best practices.

Deciding How Many Images You Need

It is best to maintain the least number of base images possible to limit maintenance complexity. Each image must be patched, updated, and maintained. Planning enables you to choose the optimal number of base images for your environment. Your VMware Horizon Cloud Service representative can help you determine what your business units, such as accounting, IT, sales, and legal departments, have in common and which business units must be siloed. Horizon Cloud Service includes up to 10 image templates with each subscription, and you can convert additional images from your standard desktop capacity. See Service Description: VMware Horizon Cloud Service with Hosted Infrastructure.

Also consider alternative methods of reducing image sprawl, such as application virtualization and application layering technologies, which allow you to abstract the application from the desktop, providing a mechanism to dynamically and instantly deliver the application to the desktop without installing or updating the application directly in the image. The application package is updated instead of the desktop image, which results in fewer images to manage.

Using Traditional or Instant-Clone Images

You can deploy virtual desktop images in Horizon Cloud Service in the following ways:

• **Traditional clones** – Also called full clones, traditional clones are independent copies of a VM that share nothing with the parent VM after the cloning operation. Ongoing operation and management of a traditional clone is typically separate from the parent VM.

• **Instant-clone desktops** – Desktops that can be rapidly assembled on demand using VMware Instant Clone Technology. Instant Clone Technology allows identical VM clones to be created quickly. This feature builds a new VM by cloning an existing, partially booted parent VM, thus significantly reducing the disk and memory requirements and I/O cost of provisioning. The instant-clone process is faster than previous desktop-cloning technology.

For most use cases, instant clones should be leveraged. Instant clones provide the ability to manage a group of desktops using a single master image. If used with User Environment Manager, you can provide a custom desktop experience for users without the burden of managing individual full-clone desktops, reducing image sprawl and operational overhead.

Traditional clones are still the preferred method for a few use cases, especially for those requiring 3D graphics. And you must use a traditional clone with all RDSH images.

Creating Images for RDSH Servers

As part of the Horizon Cloud Service offering, VMware provides one RDSH server and guides you through the basic image life cycle for an RDSH server. The life cycle includes methods of putting the RDSH server in install mode, installing applications on it, and moving forward into publish mode. After moving into publish mode, you can turn the RDSH server into an image from which you can deploy the remote applications that you just installed. You can also use RDSH images to provide RDS session desktops. The Horizon Cloud Advanced Onboarding packages can assist you with completing this process for two to three applications so that you are confident to do more on your own. For more information, see the VMware Horizon Cloud Service Hosted Infrastructure Advance Onboarding datasheet.

If you have business units that should have exclusive access to specific applications, such as HR or finance departments, or applications that require isolated segregation, such as SAP, it is recommended that you configure separate RDSH images for each department or application to maintain the necessary isolation.

Understanding Dedicated, Floating, and Session Desktops

Horizon Cloud Service supports dedicated, floating, and session desktops. Floating (nonpersistent) desktops are recommended in a Horizon Cloud Service implementation because they require less time, maintenance, and expense than the other options.

• **Dedicated (persistent) desktops** – A virtual desktop is assigned to users the first time they log in, and they use the same virtual desktop for subsequent logins. Like a physical computer, changes made to a persistent desktop stay with that desktop. You might choose to provide persistent desktops to developers who need to install their own software on their VMs. However, for most use

cases, persistent desktops require more time to build, more effort to manage, and are more expensive.

• **Floating (nonpersistent) desktops** – A virtual desktop is assigned to users each time they log in, so users do not use the same virtual desktop for subsequent logins. When a user logs out, the nonpersistent desktop resets to a pristine state and changes to the desktop are lost. However, changes can be preserved by using profile management and folder redirection. For updating and patching, you update the image and push the update to the desktop assignment. For most use cases, nonpersistent desktops are the most convenient solution.

• **Session (shared) desktops** – An RDSH published desktop that is shared across multiple users. Also commonly known as a session-based desktop. Shared desktops should be locked down, and users should not be allowed to make system changes or install applications. For user-based changes, you can use User Environment Management and folder redirection to preserve settings. For image updates and patch management, you can update the image and push the update to the RDSH published desktop assignment.

Choosing 3D Graphics Options

You can leverage the power of GPU-acceleration for any application on any device using the following methods of 3D graphics acceleration:

• **Soft3D** – Available in the Professional, Premium, and Performance desktop models, along with shared Hosted Application Servers in Horizon Cloud Service. Soft3D provides software-accelerated graphics and allows you to run DirectX 9 and OpenGL 2.1 applications without a physical GPU. Use this feature for less demanding 3D applications, such as Windows Aero themes, Microsoft Office 2010, and Google Earth.

• **Graphics Workstations** – For more high-end 3D needs, including advanced, graphics-rich applications, Horizon Cloud Service offers Graphics Workstations backed with NVIDIA GRID vGPU. Horizon Cloud Service brings workstation-class performance to remote and mobile workers even over high-latency networks just like any other desktop. Note that 3D graphics applications typically have different bandwidth requirements than traditional office worker applications. Work with the VMware Horizon Cloud Service team to define your specific bandwidth requirements.

All required NVIDIA licensing and requisite hardware are included in the price of Graphics Workstation. For more information, see the Service Description for the VMware Horizon Cloud Service. For more information about NVDIA GRID with Horizon 7, see Horizon 7 with Blast 3D.

Staggering Automatic Antivirus Updates

Horizon Cloud Service does not include an antivirus solution. You can use the solution that you already have by obtaining additional licenses for the Horizon Cloud Service environment. However, this is not a Horizon Cloud Service requirement.

If you choose to use an antivirus solution on your Horizon Cloud Service desktops or RDSH servers that updates DAT files, it is best to stagger the updates across your environment. Doing so protects you from using all the resources in your environment to update all your VMs at the same time, which could result in slower performance.

In addition to staggering antivirus updates, it is best to use a fixed schedule that avoids large concurrent updates, such as updating outside of normal business hours or creating a maintenance window. Avoiding large concurrent updates also prevents using all resources at the same time, which can slow performance.

Assigning Applications

Horizon Cloud Service with Hosted Infrastructure offers two methods of delivering applications: remote applications and native applications.

Managing Remote Applications

Remote applications are installed on RDSH servers and seamlessly delivered through the Horizon Client or Horizon Cloud Service User Portal. Users see an application that appears to be natively integrated with their local desktop, but it is actually delivered from the cloud. Windows applications hosted on RDSH servers can be delivered to non-Windows platforms, such as Android and iOS.

Assigning remote applications allows you to publish applications using RDSH servers that are based on an RDSH image, also called published applications, or RDSH-hosted applications. To create a remote application assignment, you select the number of RDSH servers to provision and the number of users per server. As you select applications to assign to users, all applications installed on the selected RDSH image are visible to you. In addition to selecting the automatically discovered applications, you can also define and

associate customized remote applications with an RDSH image in your application inventory.

Image Management Strategies

Consult your image management team about developing good profile, patch, and backup management practices. Involving representatives from your image management team in decision-making and deployment early enables them to ask questions, voice concerns, and address issues, and helps avoid unexpected problems. Consult your image management team about the following (see the navigation bar on the left):

• Profile management

• Patch management

• Backup management

Profile Management

User profiles are an important part of desktop images. A user profile consists of the folders, files, and configuration settings that are unique to a specific user. Setting up user profiles, choosing whether to assign users to persistent or nonpersistent desktops or RDSH servers, and deciding when to use redirection are all part of image management.

In a virtual environment, user profiles are typically stored on a server instead of on a physical desktop. That way, the user profile data follows the user from desktop to desktop. When thinking about profile management in a virtual environment, it makes sense to start with assignments. Horizon Cloud Service has desktop assignments for dedicated, floating, and session-based desktops, along with remote applications.

• **Traditional-clone, dedicated (persistent) desktops** – A virtual desktop is assigned to the user the first time the user logs in, and the user uses the same virtual desktop for subsequent logins. Users can customize the virtual desktop and use it to access their documents and applications. For users with a single, persistent desktop, the user profile can be stored directly on their desktop. Changes that the user makes are maintained on the same virtual desktop. However, consider storing user profiles on a server to preserve changes in case the virtual desktop becomes corrupt or the user also accesses remote applications.

• **Instant-clone, dedicated (persistent) desktops** – This assignment is similar to a persistent traditional clone in that the user uses the same virtual desktop computer name for all logins. The difference is that the virtual desktop is refreshed to a pristine state when the user logs out, and all changes are lost. To provide a persistent-like experience, the user profile must be stored on a server.

• **Traditional-clone and instant-clone, floating (nonpersistent) desktops** – A new virtual desktop is assigned to users each time they log in, so they do not necessarily use the same virtual desktop for subsequent logins. A user cannot customize a specific desktop or add documents or applications to it, because the disk is refreshed to a pristine state when the user logs out, and all changes are lost. However, changes can be preserved by storing the user profile on a server. For users with multiple desktops or who access remote applications, the user profile follows the user and is available at each desktop or remote application access so that the user's experience remains consistent.

• **Traditional clone, session (shared) desktops and remote applications** – Users are connected to the RDSH server with the fewest amount of connections, so they do not necessarily use the same server for subsequent logins. The RDSH server should be locked down, and users should not be allowed to make system changes or install applications. To preserve changes and provide a consistent user experience, store the user profile on a server.

Deciding What to Redirect

You can provide a persistent-like user experience on nonpersistent desktops by using redirection with user profiles. Users get the same application settings and files when they log in, no matter which nonpersistent desktop they use. With redirection, your users enjoy the advantages of persistent desktops for the cost of nonpersistent desktops.

To use redirection, identify the resources your users need to do their work, determine where your users save their work, and decide how much of their work you want to redirect. For example, you can choose to redirect everything that your users save to their desktops or My Documents folder to a file share. Giving users access to the file share makes their work always available to them, no matter which desktop assignment or remote application they use. You can also redirect backgrounds, screensavers, configurations for Outlook, and so on. Another option is to train your users to save all their work to a file share themselves, thus doing the work of redirecting.

Deciding How to Redirect

VMware User Environment Manager is a good way to manage redirection. User Environment Manager is the critical component of JMP that supports user-centric computing and addresses end-to-end application and user management. You can set up User Environment Manager to work with Horizon Cloud Service to help you manage user personas across devices and locations. Instead of focusing on the user's device, User Environment Manager focuses on the user's context, such as the user profile, personalization settings, application settings, contextual policy settings, user rights, licensing, and reporting settings.

Deciding Where to Redirect

When you use redirection to store user profiles, the user profile is redirected to a new permanent location. You have three possible locations to redirect user profile information:

• **Redirect to the same location as the virtual desktops and RDSH servers (recommended)** – You can redirect the user profile to a file server in the same location as the virtual desktops and RDSH servers by using a utility server. The profile data never leaves your Horizon Cloud Service tenant. For performance and security reasons, this option is best. When using User Environment Manager with Horizon Cloud Service, a utility server is required to store the user profile.

• **Redirect to an infrastructure-as-a-service (IaaS) instance** – You can redirect user profiles to a file server in the same physical data center as the virtual desktops and RDSH servers. These resources can be in a separate virtual data center using IaaS provided by the Horizon Cloud Service provider. An IPsec tunnel can be used to connect the two virtual data centers.

• **Redirect across the VPN** – You can redirect the user profile across your VPN to a file server in your main data center. Latency and bandwidth are key factors in successfully redirecting back to your data center.

Patch Management

It is important to establish good patch management practices. You might need to alter your existing patch management process based on the type of assignment you use:

• **Traditional-clone, dedicated (persistent) desktops** – You must push out application updates to each VM as you would to a physical desktop or use a third-party utility and also patch the image itself.

• **Instant-clone, dedicated (persistent) desktops** – Because these assignments do not retain changes between sessions, image patching and application updates are straightforward. Patch the image, and then refresh the assignment by pushing or reassigning the image. To patch or update an application installed on the image, update the application inside the image and then push or assign the image.

• **Traditional-clone and instant-clone, floating (nonpersistent) desktops** – These desktops do not retain changes between sessions, so image patching and application updates are straightforward. Patch the image, and then refresh the assignment by pushing or reassigning the image. To patch or update an application installed on the image, update the application inside the image and then push or assign the image.

• **Traditional-clone, session (shared) desktops and remote applications** – Update by patching the image, and then refresh the assignment by pushing the image. To patch or update an application install on the image, update the application inside the image and then push the image.

Turning Off Automatic Update Features

Many applications have an auto-update feature that periodically updates the application. These automatic updates are lost when a user logs out of a traditional- or instant-clone nonpersistent desktop or an instant-clone persistent desktop. It is recommended that you turn off this feature for these types of desktop assignments.

Testing Patches and Updates on Subset Pools

When introducing a major change, such as large upgrades, installations, new applications, application updates, or service packs, it is recommended that you first test the change on a subset desktop or application assignment. Create a copy of your image so that if the changes cause problems, you can return to the original.

Duplicate an image in the Horizon Cloud Service Administration Console. Then apply the service pack, upgrade, or other major change to the copy. If problems occur, you can duplicate the original image again. If the change is successful, you can apply the changes to your primary production assignments.

Backup Strategies

It is important to establish good backup practices. Include representatives from your backup and desktop teams in the decision-making and deployment from the start to address questions, concerns, and issues early

Supporting Many Backups of Images

Horizon Cloud Service with Hosted Infrastructure allows you to keep two backups of any given image. If you want more than two backups, you must manage subsequent backups manually. It is recommended that you create a management pool with several VMs to copy, back up, test, and verify success whenever you make changes to the image.

Backing Up Before Changes

Before making changes to an image, it is recommended that you create a backup so that if something breaks while making changes, you can revert to the previous image. Create one basic image, copy it several times, and modify one copy for each business unit, such as one for your financial department, another for your operations department, and so on. Then back up all images before the change so that you can revert if needed.

Always Testing Changes

Any changes to your infrastructure, whether patches, upgrades, additions, or subtractions, affect the infrastructure, sometimes in unforeseen ways. Additions can break the system and damage the image, and new patches can conflict with existing applications on the desktops. Therefore, it is important to test each time you make a change. To verify that your changes have not had an adverse effect, change and test a small subset of desktops before applying the change to all your production assignments. User acceptance testing can be included as one of the steps in your testing process.

Backing Up After Successful Changes

Back up again after making successful changes to an image so that if something goes wrong after a future change, the image can be reinstated in the future.

To back up images, you can set up a management assignment specifically for backups and copies of images and add VMs to the pool to use for testing and backup purposes. Restoration is then a matter of reverting to another VM in the management assignment, which is based on a previously successful image.

Creating RDSH Management Pools

Horizon Cloud Service with Hosted Infrastructure supports hosted applications, so you might have RDSH servers to manage as well as desktop assignments. The backup recommendations are the same for RDSH servers.

Additional Resources

You can find out more about Horizon Cloud Service from the following resources:

- VMware Horizon Cloud Service with Hosted Infrastructure product page
- VMware Horizon Cloud Service with Hosted Infrastructure Support Center
- Moving Virtual Desktops to the Cloud
- Horizon DaaS (Desktop as a Service) Platform for Service Providers (formerly Desktone)
- Horizon 6 with PCoIP—Up to 30% Bandwidth Savings out of the Box
- VMware Horizon 6 with View Performance and Best Practices
- VMware User Environment Manager
- VMware OS Optimization Tool
- VMware Horizon Cloud On-Premises Infrastructure
- Service Description VMware Horizon Cloud Service with Hosted Infrastructure
- VMware Horizon Cloud Service with Hosted Infrastructure Terms Of Service

• VMware Horizon Cloud Service Hosted Infrastructure Advanced Onboarding

About the Authors and Contributor

This document was written by

• Rick Terlep, End-User-Computing Architect, End-User-Computing Technical Marketing, VMware

• Jerrid Cunniff, End-User-Computing Cloud Services Senior Solutions Engineer, VMware

• Justin Venezia, Senior Architect, End-User-Computing Cloud Services, VMware

• Joan Mealey, VMware alumna

• Simon Le Comte, Director, End-User-Computing Cloud Services Architect Team, VMware

• Cindy Heyer Carroll, Technical Writer in End-User-Computing Technical Marketing, VMware

• Josue Fontanez, VMware alumnus

• Ian Hadfield, Senior Services Engineer, DaaS Operations, VMware

• Stacy Malcolm, DaaS Deployment Engineer, Professional Services Organization, VMware

• David Ryder, Horizon Cloud Service with Hosted Infrastructure Senior Solutions Engineer, DaaS Professional Services Organization, VMware

• David Gilon, Product Line Manager, Desktop Product Management, VMware

• Stéphane Asselin, Senior Manager, Product Engineering, VMware

• Jonathan Spence, Senior Technical Writer, DaaS R&D, VMware

The following individual contributed significantly to updating this document:

Charlie Rizor, VMware alumnus

Feedback

The purpose of this document is to assist you. Your feedback is valuable. To comment on this document, contact VMware End-User-Computing Technical Marketing at euc_tech_content_feedback@vmware.com.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com