VMware Horizon Cloud Service on Microsoft Azure Security Considerations

vmware®

Table of Contents

Executive Summary

This white paper provides security details related to VMware Horizon® Cloud Service™ on Microsoft Azure. The paper discusses the architecture of the service, the different components and their respective ownership, networking, and cloud connectivity. The document also describes the different types of data stored, including sensitive and personally identifiable information (PII), and the available access to that data.

Audience

The information in this document is intended for experienced data center IT administrators with knowledge of Microsoft Azure, virtualization technology, and networking.

Introduction

Horizon Cloud Service on Microsoft Azure is a software service from VMware that enables the delivery and management of virtual desktops and applications on Azure. Horizon Cloud on Microsoft Azure allows you to bring your own existing Azure infrastructure capacity and pair it with the Horizon Cloud Service. Built from the ground up as a cloud-native, multi-tenant solution, Horizon Cloud on Microsoft Azure combines the benefit of consuming desktop and application virtualization as an always up-to-date, software-as-a-service from VMware with the consumption-based infrastructure pricing and extensive global footprint of Azure.

Architecture

The Horizon Cloud Service is delivered via the VMware Horizon Cloud control plane that VMware hosts and maintains in the cloud. The control plane enables the central orchestration and management of virtual desktops and apps in your Microsoft Azure capacity. The cloud control plane also hosts a common management user interface referred to as the Horizon Cloud administration console.

Horizon Cloud allows you to connect your Azure infrastructure to the control plane and securely deliver virtual desktops and apps hosted in any of the supported globally located Azure regions.

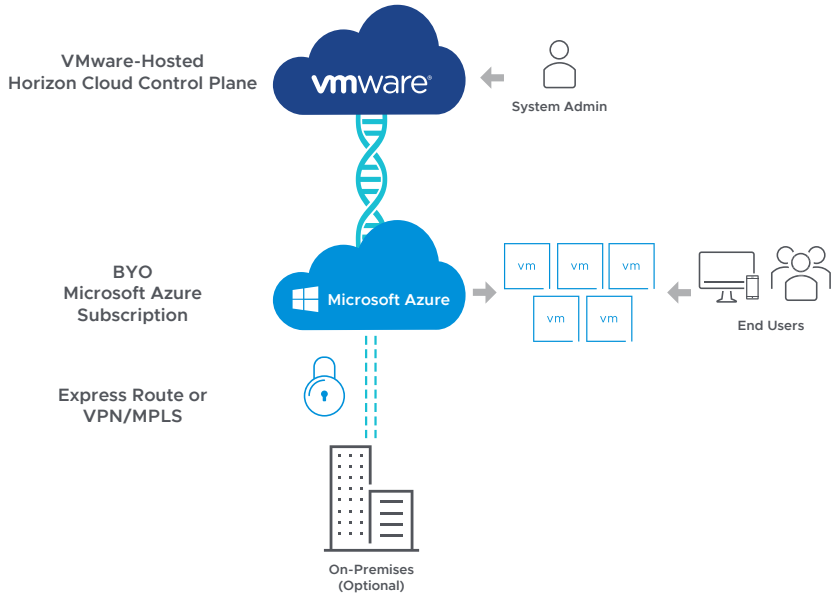

Figure 1: Horizon Cloud Service on Microsoft Azure

Architecture Components

The key components of Horizon Cloud Service are the Horizon Cloud control plane and Horizon Cloud pods.

Horizon Cloud Control Plane

The Horizon Cloud control plane enables the central orchestration, management, and monitoring of the virtual desktops and apps in your Azure capacity.

- There are multiple instances of Horizon Cloud control plane—one in the U.S., one in EMEA (Germany), and one in Australia. These different control plane locations allow organizations to keep their data local to their geography of choice to meet compliance and data locality requirements, if necessary.
- When your organization subscribes to the Horizon Service, a subscription account is created and mastered in the Horizon Cloud control plane in the U.S. Outside of the initial account creation and management, an organization is always paired to only one of the control plane instances. For example, in Figure 2, Organizations 1 and 2 are paired with the U.S. control plane instance, Organization 3 is paired with the control plane in EMEA, and Organization 4 is paired with the control plane in Australia. In other words, an account cannot be paired with multiple control plane instances.
- Any data for an organization is maintained solely within the control plane region selected for that account, including service logs.
- Organizations can choose the control plane location to pair with. Typically, this decision is governed by the need for data locality and sovereignty.
- Workloads can be run in any supported region, not only in regions with a control plane. For more information, see *Horizon Cloud Pod(s)*.

Horizon Cloud Pod(s)

Every organization that subscribes to the Horizon Cloud Service may deploy one or more Horizon Cloud pods.

- A pod is a logical construct that defines a unit of Azure infrastructure capacity that the Horizon Cloud Service pairs with.
- You can select any of the supported Azure regions to deploy the pod(s).
- There is no restriction on where a pod is located with respect to the control plane location. In other words, while you may choose to pair with the Horizon Cloud control plane in EMEA, the connected pods may be located in any Azure regions globally.

Multi-Tenant Service

Horizon Cloud Service is a multi-tenant cloud service. A subscription to the service is a tenant of the service. An organization that subscribes to the service is a tenant.

An organization is paired with only one Horizon Cloud control plane instance at any time. However, an organization can have multiple pods spread globally across any of the Azure regions.

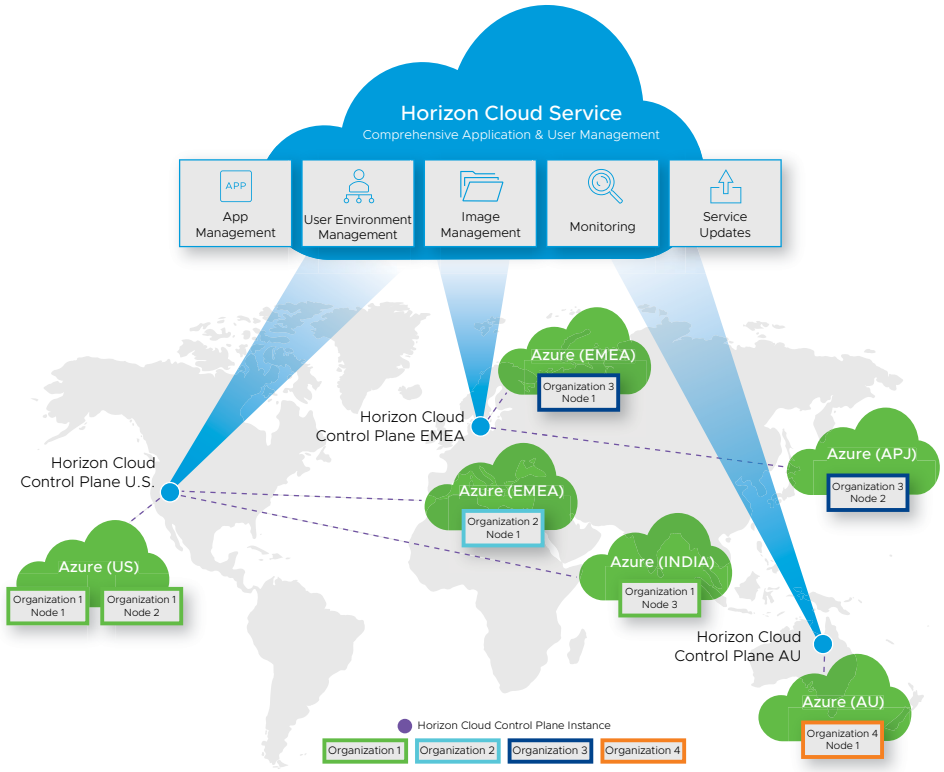

Figure 2: Example Showing Organizations 1, 2, 3 and 4 Subscribed to the Horizon Cloud Service

Component Ownership

When you subscribe to the Horizon Cloud Service, you are responsible for providing the following items:

- Valid Microsoft Azure subscription – You are responsible for completing the prerequisites as described in the *VMware Horizon Cloud Service on Microsoft Azure requirements checklist*.
- File storage (on premises or in Azure)
- Active Directory or Azure AD Domain Services
- Windows OS licenses
- RDS CALs
- Master image and applications to publish
- Optional VPN/ExpressRoute connectivity to the on-premises corporate network

VMware will provide:

- Horizon Cloud service delivered via the control plane
- Horizon Cloud Administration Console
- Secure connectivity between the control plane and Azure
- Automatic pairing between the control plane and desired Microsoft Azure Regions and subsequent deployment of pod(s) in the Azure regions
- Remote access for end users to virtual desktops and applications via VMware Unified Access Gateway™
- Internal access for end users to virtual desktops and applications via VMware Unified Access Gateway
- VMware Workspace ONE® Access for end-user access to virtual desktops and applications
- Service updates
- Support

Deployment of the Horizon Cloud Pod

In order to successfully deploy your pod into Azure, you must configure your firewalls to allow Horizon Cloud to access the Domain Name Service (DNS) addresses it needs. In addition, your DNS must resolve specific names. You must ensure the DNS names are resolvable and reachable from the pod's management and tenant subnets using specific ports and protocols. Horizon Cloud uses specific outbound ports to securely download the pod software into your Microsoft Azure environment and so that the pod can connect back to the control plane. You must configure your network firewall such that Horizon Cloud has the ability to contact the DNS addresses on the ports that it requires. Otherwise, the pod deployment process will fail. Please see *DNS Requirements for a Horizon Clod Pod in Microsoft Azure* for more information.

Once you are ready to deploy a pod, you will specify your Microsoft Azure subscription details along with network-related information in the Horizon Cloud administration console. Once complete, the pod deployment service is automatically initiated via the control plane. A transient Linux VM, called the *Deployment Engine,* is deployed in the Azure subscription, which initiates an outbound request to the control plane to orchestrate the download and deployment of the pod within the provided Azure subscription. The transient VM is then deleted after the deployment.

Figure 3 illustrates the internal components of the Horizon Cloud pod. Note that only an external-facing Unified Access Gateway is shown. If an internal-facing Unified Access Gateway is required, two more VMs (without the public IP) can be deployed.

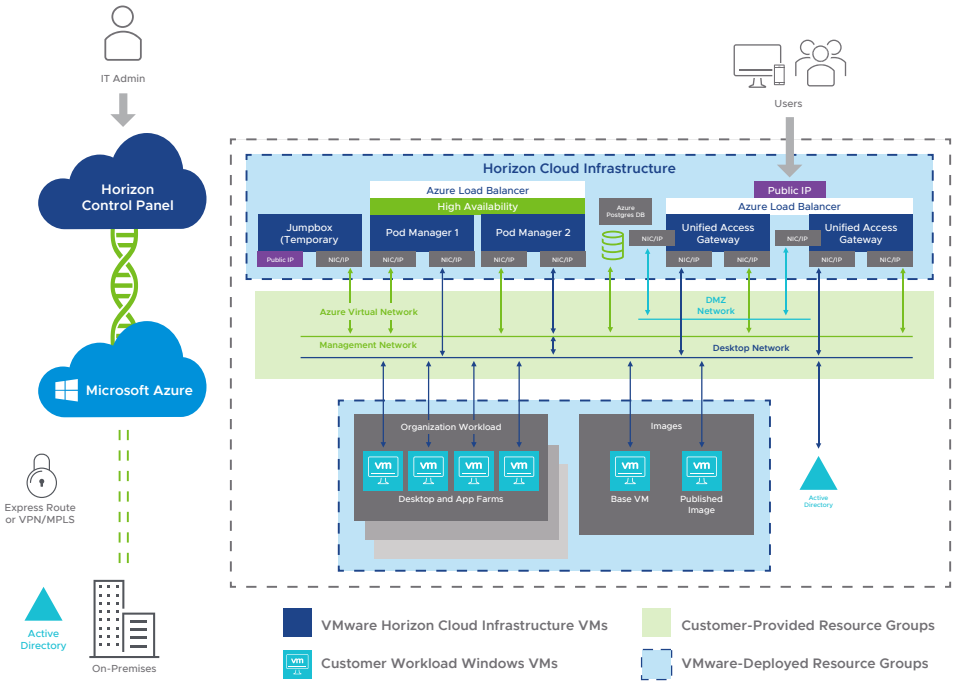

Figure 3: Horizon Cloud Pod Deployment in Microsoft Azure

Connectivity Between Horizon Cloud Control Plane and Microsoft Azure

Each pod maintains a management connection to the Horizon Cloud control plane. This connection is outbound from the pod to the control plane. There is no requirement for a VPN connection. There is no requirement for inbound management connectivity to a pod from the Internet. The control plane can use this connection to access the pod, enabling

- Configuration changes
- Live state queries
- Supportability requests, including interactive support, log fetching, and component health queries

This management connection is protected using TLS 1.2 and authenticated using strong, periodically rotated keys.

The pod makes outbound connections to the control plane over the Internet. These connections are protected by TLS 1.2 to ensure the identity of the target service and protect the content of the communication. The pod authenticates to the control plane using periodically rotated authentication tokens.

Networking

Figure 3 illustrates the networking between the different components. These can be best explained as follows:

- Cloud components
  - The IT administrator using the service, external end users, control plane, and the Azure API are all on the Internet.
  - The control plane accepts inbound requests from the IT administrator along with the pods and makes outbound calls to the Azure API.
- Horizon Cloud Pod on Microsoft Azure – The pods use three networks to connect components:
  - DMZ – Enables inbound traffic from the Internet to the external Unified Access Gateways. Network Security Groups (NSG) that are a feature of Microsoft Azure are used to inbound control access and allow only the required ports and protocols to the external Unified Access Gateways.
  - Management – An internal management network, allowing the Pod Managers to control the Unified Access Gateways and providing an outbound Internet channel for connection to the control plane and the Azure API. There is no inbound networking connectivity to this network.
  - Desktop – Customer-controlled network for the VDI desktops and RDSH servers (supporting both multi-session desktops and applications), internal Unified Access Gateways, and Pod Managers (user-facing interface).
- On-premises corporate network
  - Horizon Cloud Service may optionally communicate to the on-premises, corporate network via a VPN or ExpressRoute connection.
  - This connection may be required if the Active Directory or user data and applications are located on premises.
  - Typically, internal end users connect to the pod over this connection.

For detailed, up-to-date information about the protocols and ports used in Figure 3, please consult with the *product documentation*. Also, detailed diagrams are available in a TechZone article entitled *VMware Horizon Cloud Service on Microsoft Azure Network Ports Diagrams*.

Data Storage and Access

The Horizon Cloud service stores and handles different categories of data. Table 1 defines each category, indicating where the data is stored, who has access to it, and how this data might have personally identifiable information (PII) implications. The PII data is further divided into

- Primary PII – Data that identifies an individual, for example, username, client IP address
- Secondary PII – Data that when combined with an identity could be considered sensitive or private, for example, login times, app launch information

WHAT	WHERE	WHO	PII IMPLICATIONS
End-user data			
Data created by end users, for example, files, user settings, and user-installed applications.	This is stored only in the VDI desktops, RDSH Servers and external services (for example, file servers) which you deploy and configure. You are responsible for the ownership, access and management of these file services and VMware has no access to this data. User data is not replicated, nor is it stored in the control plane.	End users access this data from within their VDI desktop sessions or RDSH app and desktop sessions. You, the "customer," have access to this data, depending on how you configure access to the VMs or external file services that are under your control. VMware does not manage nor access this data.	Because this data is authored by end users, it may contain PII data. You have full control of where this data is stored. The disk images storing this information may be encrypted.

WHAT	WHERE	WHO	PII IMPLICATIONS
End-user usage data			
Data about the end users' usage of the system, for example, login times, application and desktop launches, VDI and RDSH performance data, VDI and RDSH server hostname, and client IP address. • This data is not collected if you disable the Horizon Cloud monitoring service (see *Monitoring* for more details). • The data is normally stored for the life of your Horizon Cloud subscription and provides historical reporting and aggregated viewing of data. • Once the monitoring service is enabled, you may further opt out of collecting user session information (Enable User Session Information = No) to reduce the long-term storage and anonymize the PII data as stored by the monitoring service.	End-user usage data is maintained both in the pods and in the control plane. • Data is explicitly stored in the pod for immediate and historic query. • Data is implicitly logged in log files as part of the operation of the system. • Data is explicitly stored in the control plane for immediate and historic query. • Data is implicitly stored in the control plane as part of administrator notifications that may identify end users.	This data is used by you to help manage your end user's experience. VMware may use this data to monitor the overall service and provide service support.	The following PII data is stored unless the Horizon Cloud monitoring service is disabled. **Primary PII** • User identity: name, username, user IDs (for example, AD SID) • Client IP address **Secondary PII** • Login timestamp • VDI and RDSH VM hostname • Application launches Both you and VMware can see both Primary and Secondary PII data. Opting in or out of Enable User Session Information determines how long the Primary PII data is stored. When disabled, this data is maintained to provide immediate service and support (for example, who is currently logged in), but this data is not stored historically (for example, who logged in last week).

WHAT	WHERE	WHO	PII IMPLICATIONS
Horizon Cloud subscription account definition			
Data about the definition of your service, for example, Active Directory configuration; Pod configuration; desktop assignments, application assignments, farm, and app definitions; entitlements to services; and assignments to services. This includes storing usernames and credentials for integrated services like Active Directory and Microsoft Azure. See *Secure Credential Storage* for more information.	This data is stored in both the pods and in the control plane.	You own this data and manage it through the Administration Console. VMware can access this data to provide support and understand the service usage. The service itself can use the supplied credentials to operate. VMware operations and support staff are not given access to stored credentials.	The following PII data is stored: • **Primary PII** – User/admin identity: name, username, user IDs (for example, AD SID and GUIDs). The main use of PII is to identify the entitlement of end users to services (VDI desktops, remote applications, AV applications, UEM policies), and the assignment of end users to resources (for example, linking an end user to a specific VDI desktop VM in a dedicated assignment). In addition, IT administrators are identified and given rights within the system.
IT administrator usage data			
Data about your usage of the system, for example, login times, and audit information tracking changes to service configuration and operations.	This data is stored in both the pods and in the control plane.	You can see audit data. VMware can access this data to provide support and understand the service usage.	The following PII data is stored: • **Primary PII** – Admin identity: name, username, user IDs (for example, AD SID and GUIDs). Audit and log data for system changes will identify the IT administrator who caused the change.

Table 1: Data Categories

Active Directory Domain Registration

After you have successfully deployed your first pod and it is successfully paired with Horizon Cloud, log in to the Horizon Cloud Administration Console to register an Active Directory domain, perform the domain join and bind, and assign the super administrator role to at least one of the groups in that domain.

The pod connects to the Active Directory domain controller on LDAP port 389 and global catalog on port 3268. LDAP connections are secured using GSSAPI/Kerberos.

There are two types of Active Directory accounts required:

- **Domain bind and domain bind aux account** – Active Directory domain bind and domain aux account (a standard user with read access) that has permission to read objects in AD. Both GSSAPI and NTLMSSP binds are used for these accounts and the Microsoft GPO of "Require Signing" is supported.
- **Domain join and domain join aux account** – Active Directory domain join and domain join aux account that has additional permissions to perform Sysprep operations and join computers to the domain, create new accounts, and more. Only GSSAPI binds are used for these accounts.

Minimal information on Active Directory groups (and their descendant groups) is cached to entitle desktop and application assignments, URL redirection assignments, and more.

When a user logs in, they are authenticated and authorized without using the cache to ensure that only the most recent data is used. Once logged in, entitlement checks are made against the cached data to ensure high performance.

Secure Credential Storage

The Horizon Cloud on Microsoft Azure service stores the following credentials for each Horizon Cloud subscription account:

- Active Directory domain bind and domain bind aux username and password
- Active Directory domain join and domain join aux username and password
- File share username and password
- Azure subscription credentials

The user credentials are protected with AES 128-bit encryption when stored in the cloud. These credentials are accessible by the Horizon Cloud service when performing operations on behalf of the account, or to distribute to components that need access.

On the pod, these credentials are stored encrypted with a per-pod key. These credentials are accessible by the pod service when performing operations on behalf of the organization.

Backup and Protection

The Horizon Cloud control plane stores data in a fully replicated cluster across multiple fault domains in the service's region. Furthermore, explicit offline backups of the data are taken and stored in region.

Monitoring

The Horizon Cloud Monitoring Service enables collection of user session information for service utilization, trending, and historical analysis. The data is used in charts on the Dashboard page and in reports on the Reports page. The data collected is regarding the end users' usage of the system, for example, login times, application and desktop launches, VDI desktop and RDSH performance data, VDI and RDSH server hostnames, client IP address, and username. You can opt out of the monitoring service at any time.

When the monitoring service is enabled, there are two modes of operation:

- Where collection of User Session Information is enabled
- Where it is disabled

You can use the Enable User Session Information toggle to enable or disable this mode at any time.

When the Enable User Session Information is disabled (Enable User Session Information: No), the system will collect user session information for a limited period and will no longer store user identities for historical queries. Instead, the data is anonymized using hashing so that certain aggregated queries are still possible to enable real-time administration, but individual users cannot be identified. In addition, the historical and aggregated viewing of that user information will be disabled. Thus, the reports that would display historical and aggregated viewing of monitoring data, such as the Session History report, becomes not available.

Note that even when Enable User Session Information is disabled, user-identifying data is stored for up to 24 hours to provide real-time support of the service. You can disable the monitoring service completely if you do not want any of the monitoring data to be stored in the cloud monitoring service at all.

Metrics Collected by Horizon Cloud Monitoring Service

The data collected by the Horizon Cloud monitoring service is collected via two main channels:

- The Desktop Agent which is running on the VM (which may be a VDI desktop or RDSH Server)
- Monitoring Service on the Pod

The data collected can be summarized into the following categories.

SUMMARY	DESCRIPTION
Collected from the VDI and RDSH by the Desktop Agent	
General	Tenant ID, Pod ID, Client Version, Server Hostname, Device Type (Desktop/Server).
CPU	Details such as interrupts/second, % of processor time spent in idle mode, user mode, and more.
Memory	Details such as rate of read/write operations to disk, average time of a read from disk, and more.
Disk	Details such as amount of physical memory, rate of pages read/write, rate of recovery of page faults.
Network Interface	Details such as the rate of packets received and sent, length of the output packet queue, ports opened, and more.
Session	Details such as time to load a profile, time to connect and disconnect, login and logout timestamp, duration of a connected session, number of handles currently opened for the session, and more.
Service Status	Status of various services like agent, firewall, VMware tools, Session Manager, and more.
Client	Horizon Client details like client ID, IP address, client protocol, client type, and more.
Firewall	Stats like protocol enabled (PCoIP/Blast), Remote Desktop enabled, and more.

SUMMARY	DESCRIPTION
Collected from the Windows Servers by the Desktop Agent	
User Information (hashed when User Session Information is disabled)	User Name, domain, Session status.
PCoIP protocol metrics	PCoIP protocol-related metrics such as estimated bandwidth for uplink and downlink, jitter, latency, bytes transmitted and received for audio, USB, ThinPrint, imaging, overall, and more.
BLAST protocol metrics	BLAST protocol-related metrics such as estimated bandwidth for uplink and downlink, jitter, latency, bytes transmitted and received for audio, USB, ThinPrint, imaging, overall, and more.
Client Keyboard/Mouse/Display	Client Display; Keyboard and Mouse details such as language, key delay, type, display type, and more.
Collected from the Pod by the Monitoring Service	
General	Tenant ID, Pod ID, Customer ID, Desktop/Application Assignment Name, ID, Type, Capacity, Apps used.

Table 2: Metrics Collected by Horizon Cloud Monitoring Service

Operational Access

In the event of troubleshooting or diagnosing an issue, VMware can

- Obtain log files and crash reports from the Horizon Cloud pod (made available as "Support Bundle"), which will show user names, times when users have accessed the system, and other environment information including IP addresses and hostnames.
- Obtain other files, such as configuration files, from the deployed infrastructure VMs within the Horizon Cloud pod.
- Have real-time access to the current operational health status of the Horizon Cloud pod.
- Have interactive shell access on the Pod Manager for troubleshooting and support.

Conclusion

The VMware Horizon Cloud Service allows you to connect your Azure infrastructure to the Horizon Cloud control plane and securely deliver virtual desktops and applications hosted in any of the globally located Azure data centers. This white paper covered many security aspects of VMware Horizon Cloud on Microsoft Azure, including architecture, components, networking, data storage, and access.

References

Horizon Cloud on Microsoft Azure Prerequisites

Getting Started with VMware Horizon Cloud Service on Microsoft Azure

Horizon Cloud Service on Microsoft Azure Administration Guide

Horizon Cloud on Microsoft Azure – Terms of Service

About the Authors

This paper was written by

- Frank Taylor, Principal Engineer, Cloud Service, VMware
- David Simons, Director, Product Development, Horizon Cloud Service, VMware
- Najaf Khan, Senior Engineer, Product Development, Horizon Cloud Service, VMware
- Griff James, Senior Engineer, Product Development, Horizon Cloud Service, VMware
- Ming Chen, Senior Manager, Product Development, Horizon Cloud Service, VMware
- Shikha Mittal, Director, Product Management, Horizon Cloud Service, VMware
- Jerrid Cunniff, Product Management, Horizon Cloud Service, VMware
- Gabe Knuth, Product Marketing, Horizon Cloud Service, VMware

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com Item No: FY20-5712-VMW-HC-MICROSOFT_AZURE-SECURITY-WP-USLET-20200111 1/20