## Table of Contents

Executive Summary ......................................................................................................................... 3  
Audience ........................................................................................................................................ 3  
Introduction ................................................................................................................................... 3  
Architecture..................................................................................................................................... 4  
  Architecture Components ................................................................................................................ 5  
  Multi-Tenant Service ..................................................................................................................... 6  
Component Ownership .................................................................................................................... 7  
  Deployment of the Horizon Cloud Node ......................................................................................... 8  
Connectivity Between Horizon Cloud Control Plane and Microsoft Azure ..................................... 8  
Networking..................................................................................................................................... 9  
  Protocols and Ports ....................................................................................................................... 11  
Data Storage and Access .................................................................................................................. 12  
  Active Directory Domain Registration ......................................................................................... 15  
  Secure Credential Storage ............................................................................................................ 15  
  Backup and Protection .................................................................................................................. 15  
Monitoring ...................................................................................................................................... 15  
  Metrics Collected by Horizon Cloud Monitoring Service ............................................................. 16  
Operational Access .......................................................................................................................... 16  
Conclusion ...................................................................................................................................... 16  
References ....................................................................................................................................... 17  
About the Authors ............................................................................................................................ 17
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 access available.

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 on Microsoft Azure is a software service from VMware that enables the delivery and management of virtual desktops and applications on Microsoft Azure. Horizon Cloud on Microsoft Azure allows you to bring your own existing Microsoft 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 Microsoft Azure.
Architecture

The Horizon Cloud service is delivered via a control plane that VMware hosts and maintains in the cloud. The control plane enables the central orchestration and management of remote desktops and applications 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 Microsoft Azure infrastructure to the control plane and securely deliver virtual desktops and apps hosted in any of the globally located Microsoft Azure data centers.

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 nodes:

Horizon Cloud Control Plane
The Horizon Cloud control plan enables the central orchestration, management, and monitoring of remote desktops and applications in your Microsoft Azure capacity.

• There are two instances of Horizon Cloud control plane—one in the U.S. and one in EMEA (Germany), with other locations expected soon. 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 Cloud 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 below, Organization 1 is paired with the control plane U.S. instance, and Organization 3 is paired with the control plane in EMEA. 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 logs of the service.
• Organizations can choose the control plane location to pair with. Typically, this decision is governed by the need for data locality and sovereignty.

Horizon Cloud Node(s)
Every organization that subscribes to the Horizon Cloud service may deploy one or more Horizon Cloud nodes.

• A node is a logical construct that defines a unit of Microsoft Azure infrastructure capacity that the Horizon Cloud service pairs with.
• You can select any Microsoft Azure data centers to deploy the node(s).
• There is no restriction on where a node 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 nodes may be located in any Microsoft Azure data center globally.
Multi-Tenant Service
Horizon Cloud 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 nodes spread globally across any of the Microsoft Azure data centers.

Figure 2: Example Showing Organizations 1, 2, and 3 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 Microsoft Azure)
• Active Directory
• Windows OS licenses
• Master image and applications to publish
• Optional VPN/MPLS 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 Microsoft Azure
• Automatic pairing between the control plane and desired Microsoft Azure data center and subsequent deployment of node(s) in the Microsoft Azure data center
• Remote access for end users to virtual desktops and applications via VMware Unified Access Gateway™
• VMware Workspace™ ONE™ portal for end-user access
• Service updates
• Support
Deployment of the Horizon Cloud Node

Once you specify your Microsoft Azure subscription details in the Horizon Cloud Administration Console, a Horizon Cloud node deployment service is automatically initiated via the control plane. A transient Linux VM is deployed in the Microsoft Azure subscription which initiates an outbound request to the control plane to orchestrate the download and deployment of the Horizon Cloud node within the provided Microsoft Azure subscription. The transient VM is then deleted.

Figure 3 illustrates the internal components of the Horizon Cloud node.

Figure 3: Horizon Cloud Node Deployment in Microsoft Azure

Connectivity Between Horizon Cloud Control Plane and Microsoft Azure

Each node maintains a management connection to the Horizon Cloud control plane. This connection is outbound from the node to the control plane. There is no requirement for a VPN connection. There is no requirement for inbound management connectivity to a node from the Internet.

The control plane can use this connection to access the node, enabling:

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

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

The node makes outbound connections to the control plane over the Internet. These connections are protected by TLS to ensure the identity of the target service and protect the content of the communication. The node authenticates to the control plane using same string, periodically rotated keys.
Networking

Figure 4 illustrates the major components of a Horizon Cloud solution. It shows how the components interact with the relevant networks, indicating the direction in which communication is initiated.
• 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 and the nodes and makes outbound calls to the Azure API.

• Horizon Cloud Node on Microsoft Azure – The node uses three networks to connect components:
  - DMZ – Enables inbound traffic from the Internet to the Unified Access Gateway.
  - Management – An internal management network, allowing the Node Manager to control the Unified Access Gateway 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 RDSH and Node Manager (user-facing interface).

• On-premises corporate network
  - Horizon Cloud service may optionally communicate to the on-premises, corporate network via a VPN, MPLS, or ExpressRoute connection.
  - This connection may be required if the Active Directory and/or user data and applications are located on premises.
  - Typically, internal end users connect to the node over this VPN.
Protocols and Ports

Figure 5 provides a schematic of the ports used between components.

In the diagram, the grey lines indicate flows, annotated with the network ports used. Ports are all TCP, unless indicated.
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

<table>
<thead>
<tr>
<th>DATA TYPE</th>
<th>WHAT</th>
<th>WHERE</th>
<th>WHO</th>
<th>PII IMPLICATIONS</th>
</tr>
</thead>
<tbody>
<tr>
<td>End-user data</td>
<td>Data created by end users, for example, files, user settings, and user installed applications.</td>
<td>This is stored only in the RDSH 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.</td>
<td>End users access this data from within their RDSH app and desktop sessions. You may have access to this data, depending on how you configure RDSH or external file services. VMware does not manage nor access this data.</td>
<td>Because this data is authored by end users, it may contain PII data. You have full control of where this data is stored.</td>
</tr>
<tr>
<td>DATA TYPE</td>
<td>WHAT</td>
<td>WHERE</td>
<td>WHO</td>
<td>PII IMPLICATIONS</td>
</tr>
<tr>
<td>------------------</td>
<td>----------------------------------------------------------------------</td>
<td>--------------------------------------------</td>
<td>----------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>End-user usage data</td>
<td>Data about the end users’ usage of the system, for example, login times, application and desktop launches, RDSH performance data, 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.</td>
<td>End-user usage data is maintained both in the nodes and in the control plane. • Data is explicitly stored in the node 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 which may identify end users.</td>
<td>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.</td>
<td>The following PII data is stored unless the Horizon Cloud monitoring service is disabled. <strong>Primary PII</strong> • User identity: name, username, user IDs (for example, AD SID) • Client IP address <strong>Secondary PII</strong> • Login times • RDS Server 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?).</td>
</tr>
<tr>
<td>DATA TYPE</td>
<td>WHAT</td>
<td>WHERE</td>
<td>WHO</td>
<td>PII IMPLICATIONS</td>
</tr>
<tr>
<td>-----------------------------------------------</td>
<td>----------------------------------------------------------------------</td>
<td>---------------------------------------------</td>
<td>---------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Horizon Cloud subscription account definition | Data about the definition of your service, for example, Active Directory configuration; node configuration; pool, 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 nodes 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).  
  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 pool). 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 nodes 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). 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 node and it is successfully paired with Horizon Cloud, you log in to the Horizon Cloud Administrator 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 node 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 account** – Active Directory domain bind 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.

- **Domain join account** – Active Directory domain join 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 RDSH 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 username and password
- Active Directory domain join 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 node, these credentials are stored encrypted with a per-node key. These credentials are accessible by the node 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, RDSH performance data, RDSH server hostname, client IP address, and user name. You can opt out of the monitoring service at any time.
When the monitoring service is enabled, there are two modes of operation—one, where collection of User Session Information is enabled and two, 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 and 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 that data, such as the Session History report, are 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 entirely if you do not want any of this data to be stored at all.

**Metrics Collected by Horizon Cloud Monitoring Service**
The data collected by the Horizon Cloud monitoring service is collected via two main channels:

- Desktop Agent on the Windows Server
- Monitoring Service on the Node

The data collected can be summarized into the following categories:

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

<table>
<thead>
<tr>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Collected from the Windows Servers by the Desktop Agent</td>
</tr>
<tr>
<td>User Information (Hashed when User Session Information is disabled)</td>
</tr>
<tr>
<td>PCoIP protocol metrics</td>
</tr>
<tr>
<td>BLAST protocol metrics</td>
</tr>
<tr>
<td>Client Keyboard/Mouse/Display</td>
</tr>
<tr>
<td>Collected from the Node by the Monitoring Service</td>
</tr>
<tr>
<td>General</td>
</tr>
</tbody>
</table>

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 node (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 node.
- Have real-time access to the current operational health status of the Horizon Cloud node.
- Have interactive shell access on the Node Manager appliance for troubleshooting and support.

Conclusion

The VMware Horizon Cloud service allows you to connect your Microsoft Azure infrastructure to the Horizon Cloud control plane and securely deliver virtual desktops and applications hosted in any of the globally located Microsoft Azure data centers. This white paper covered many security aspects of VMware Horizon Cloud Service 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
VMware 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, Horizon Cloud Service, VMware
• Shikha Mittal, Director, Product Management, Horizon Cloud Service, VMware