Service Description

VMware Horizon® Cloud Service™ on Microsoft Azure®

Last Updated: 13 September 2019

As used in this Service Description, “VMware”, “we”, or “us” means VMware, Inc., a Delaware corporation, if the billing address for your order is in the United States, or VMware International Unlimited Company, a company organized and existing under the laws of Ireland, if the billing address for your order is outside the United States. Terms not defined in this Service Description are defined in the Terms of Service or elsewhere in the Agreement.

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

Table of Contents

1. INTRODUCTION

VMware Horizon® Cloud Service™ on Microsoft Azure ("Horizon Cloud Service on Microsoft Azure" or the "Service Offering") is a cloud service offering hosted by VMware that enables the delivery of virtual desktops and applications to end users on any device, anywhere, on Microsoft Azure.

1.1 OVERVIEW

Horizon Cloud Service on Microsoft Azure is offered as a VMware subscription service and includes (a) software that allows the deployment and use of desktops and applications hosted on your Microsoft Azure infrastructure capacity and (b) access to the VMware-hosted cloud control plane via the management console ("Horizon Cloud Manager") to orchestrate and manage the virtual workloads. The software includes components that are in the VMware-hosted cloud control plane and components that are downloaded to your Microsoft Azure infrastructure capacity. The VMware cloud control plane is hosted on servers located in the United States of America, Germany, and Australia.

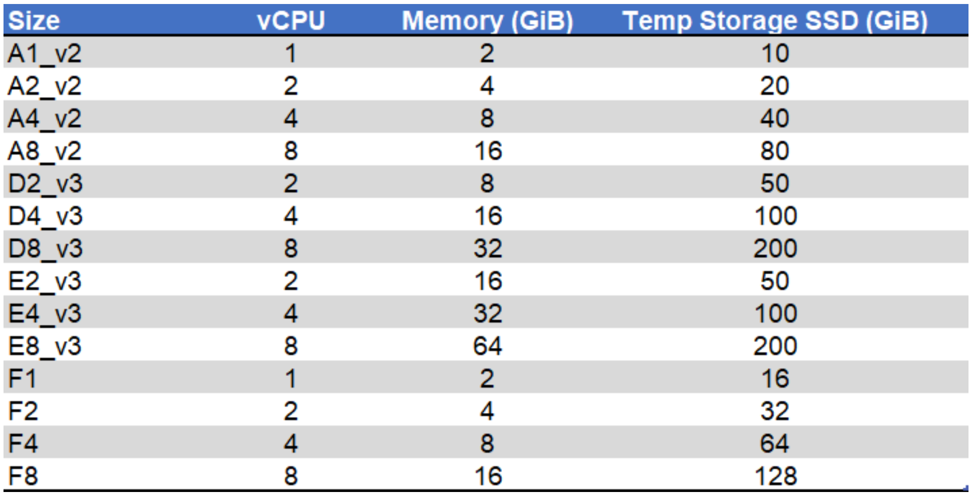
The Service Offering allows customers to purchase Horizon Cloud Desktops and Horizon Cloud Apps capacity on a 1-, 12-, 24-, 36-, -48, or 60-month subscription. It is offered in quantities of 50 seats for initial purchases, and quantities of 10 seats for incremental (add-on) purchases.

You will need to provide your own Microsoft Azure infrastructure capacity. During the onboarding of the Service Offering, the required VMware Horizon Cloud software is automatically deployed into your Microsoft Azure capacity. The deployed VMware software creates an appropriately configured entity, called a "Horizon Cloud Node" (or "Node"), which pairs with the VMware cloud control plane. After the Node is deployed, you can use the Horizon Cloud Manager to create virtual desktop assignments and RDS hosts, called "Farms", and entitle desktops and applications to your end users. You will need to size the Microsoft Azure infrastructure capacity appropriately, based on your anticipated desktop and application workload. For an optimal experience, it is strongly recommended to avoid running other non-desktop and application workloads in the specified Azure capacity at the same time.

[CONTINUED ON THE NEXT PAGE]

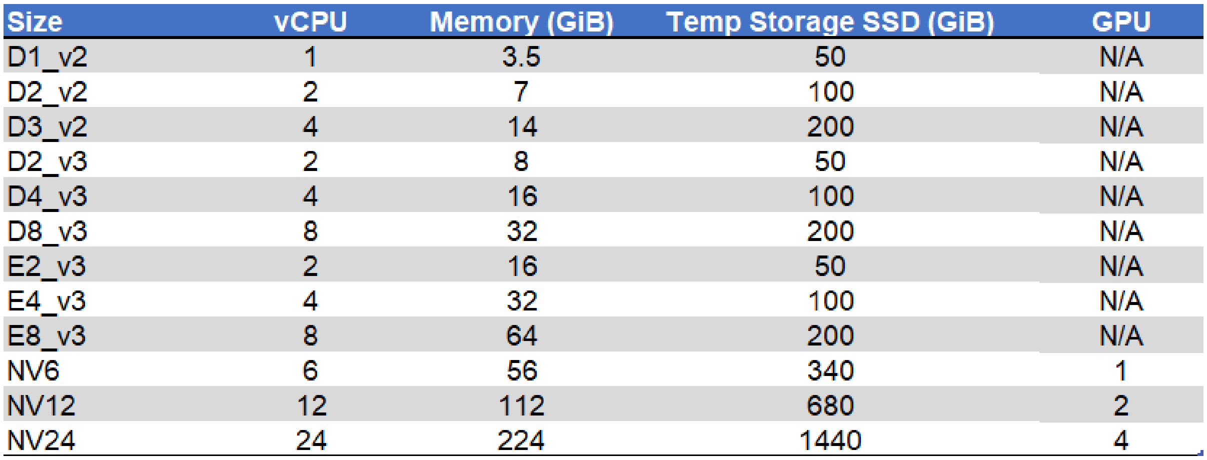
Horizon Cloud Service on Microsoft Azure supports six different series of Microsoft Azure VM Instance types for virtual desktops and Farms across Azure's global regions.

Virtual Desktops:



Size	vCPU	Memory (GiB)	Temp Storage SSD (GiB)
A1_v2	1	2	10
A2_v2	2	4	20
A4_v2	4	8	40
A8_v2	8	16	80
D2_v3	2	8	50
D4_v3	4	16	100
D8_v3	8	32	200
E2_v3	2	16	50
E4_v3	4	32	100
E8_v3	8	64	200
F1	1	2	16
F2	2	4	32
F4	4	8	64
F8	8	16	128

Farms:



Size	vCPU	Memory (GiB)	Temp Storage SSD (GiB)	GPU
D1_v2	1	3.5	50	N/A
D2_v2	2	7	100	N/A
D3_v2	4	14	200	N/A
D2_v3	2	8	50	N/A
D4_v3	4	16	100	N/A
D8_v3	8	32	200	N/A
E2_v3	2	16	50	N/A
E4_v3	4	32	100	N/A
E8_v3	8	64	200	N/A
NV6	6	56	340	1
NV12	12	112	680	2
NV24	24	224	1440	4

During your Subscription Term, you can provision any mix of applications and desktops up to the total quantity of seats purchased. The number of desktops that can be hosted will vary on the selected desktop model, the virtual machine ("VM") instance type, and the hardware resource capacity available within your current Microsoft Azure limits, up to a recommended maximum of 2,000 concurrent connected sessions per Horizon Cloud Node.

For all VM operating system ("OS") licensing, you must use your own licenses purchased through your Microsoft licensing distributor. See Appendices B and C for details on supported Guest OS and Microsoft licensing guidance.

The desktops and applications can be accessed via the VMware Horizon® Client™ or via any Web browser. Use of the desktop and mobile clients to access the Service Offering is governed by the standard VMware end user license agreement which incorporates the VMware Product Guide, copies of which are available at http://www.vmware.com/download/eula.

1.2 HORIZON CLOUD IDENTITY MANAGER

The VMware Horizon® Cloud Service™ includes the VMware Identity Manager™ feature. With VMware Identity Manager, you can set up single sign-on ("SSO") for Horizon Cloud apps and desktops, ensure security with multi-factor authentication (including VMware Workspace ONE® Verify, VMware's multi-factor authentication solution included in the VMware Identity Manager feature that is powered by a third-party service provider), and control conditional access. If you opt to use Workspace ONE Verify, then VMware, its affiliates, and its third-party service provider will have access to your personal information, including the name, phone number and email address of individual users. You are responsible for compliance with applicable laws. VMware, its affiliates and service providers will use the personal information collected through Workspace ONE Verify to provide the multi-factor authentication service. Information collected by VMware may be transferred, stored and processed by VMware in the United States or any other country in which VMware or its affiliates or service providers maintain facilities.

Use of VMware Identity Manager within the Service Offering requires a VMware Identity Manager connector, which is installed and managed on a customer-owned VM.

The VMware Identity Manager feature within Horizon Cloud may only be used for SSO, identity federation, multi-factor authentication, and app catalog access for your Horizon Cloud apps and desktops. If you want to use VMware Identity Manager with other apps such as Horizon 7 apps and desktops, SaaS apps, or mobile apps, please consult with your VMWare End User Computing ("EUC") Sales Engineer to purchase the appropriate entitlement.

If you have previously purchased a VMware Identity Manager on-premise license for general use, and the version of VMware Identify Manager is compatible with the Service Offering, we will support use of that VMware Identity Manager feature for your Horizon Cloud apps and desktops. Please consult with your EUC Sales Engineer regarding your planned use of your existing on-premise VMware Identity Manager entitlement with the Service Offering.

1.3 SERVICE OFFERING CAPABILITIES

The Service Offering includes the following capabilities:

- **Pairing** of the Microsoft Azure infrastructure capacity with the VMware cloud control plane via the automatic build-out of the Horizon Cloud components on Microsoft Azure infrastructure capacity and subsequent configuration through the VMware Horizon® Cloud Manager™.
- **Domain Binding** via the VMware Horizon Cloud Manager to set up active directory, administrator roles and permissions, and end user groups.
- **Desktop master image / gold pattern creation** and management via the ability to import a supported Windows server image from the Microsoft Azure Marketplace as a base operating system VM to which the necessary Horizon Cloud agents are automatically applied.
- **RDS Server Farms management** via the Horizon Cloud Manager, where groups of one or many server Farms are run on Microsoft Azure infrastructure to host the published desktops and applications, respectively.
- **Remote App Definition** via the Horizon Cloud Manager, where the Master Image is scanned for applications that will be published for end users.
- **Desktop assignment** via the Horizon Cloud Manager, where each assignment specifies the desktop type, Dedicated, Floating or Shared, on Microsoft Azure that will host the desktop and the gold pattern that is applied.
- **Application assignment** to one or more users via the Horizon Cloud Manager, where each assignment specifies the application Farm on Microsoft Azure that will host the applications users can access.

- **Integration with User Customization** that allows end user environments to be customized as desired. This can be enabled through a separate VMware User Environment Manager™ (UEM) console.
- **Power Management** of Microsoft Azure infrastructure capacity through the Horizon Cloud Manager, so capacity usage is tracked and managed.
- **Optional Remote access** via automatic deployment of a pair of VMware Unified Access Gateway™ instances on Microsoft Azure.
- **Optional Internal access** via automatic deployment of a pair of Unified Access Gateway instances on Microsoft Azure.
- **End user access** to the hosted desktops and applications over internal and external networks via the Horizon Client or a Web browser.
- **Optional Workspace ONE** integration via the VMware Identity Manager, which allows end users identity-based catalog access to their assigned desktops and applications.
- **Virtual Machines (VMs)** are the desktops that are accessed by the end users.

1.4 Service Offering Inclusions

The items included in the Service Offering are as follows:

Horizon Cloud on Microsoft Azure	
Horizon Cloud on Microsoft Azure software	Virtualized application and desktop delivery with RDS-hosted applications and desktops published on BYO Microsoft Azure infrastructure capacity
Horizon Cloud Manager cloud access	VMware Cloud-hosted management
Horizon Client	Application that allows end users to connect to the virtual desktop from client end points
Unified Access Gateway	Optional virtual appliance that allows secure remote access to end user computing resources by authorized users connecting either externally and/or internally.
DaaS Agent	Set of agents installed on all the virtual desktops to communicate with the back-end platform.
Horizon Agent	
User Environment Agents	
User Environment Manager	Stand-alone console for User Environment Manager.
VMware Identity Manager	Optional service that allows for single sign-on (SSO) for Horizon Cloud apps and desktops, ensure security with multi-factor authentication and control conditional access

1.5 Console Access

The Service Offering includes access to two self-service consoles:

- **My VMware Account Management Console ("My VMware™")** provides access to subscription status, integrating navigation, viewing and management of all VMware product licenses and support under a single account. It also allows you to download the Horizon Cloud on Microsoft Azure software components such as Agents, etc.
- **VMware Horizon Cloud Manager ("Console")** is the primary interface for consumption and management of the Service Offering, including domain binding, gold pattern management, desktop provisioning, application provisioning, user customization provisioning, end user entitlement, and other management operations.

1.6 Additional Information

Technical Documentation and Training

Online help outlining Key Concepts with usage examples, an "Install guide", and an "Admin Guide" is available.

Legal Terms

Use of the Service Offering is subject to the Terms of Service located at https://www.vmware.com/download/eula.html.

2. Service Operations

The following outlines VMware's roles and responsibilities in the delivery of the Service Offering. While specific roles and responsibilities have also been identified as being owned by you, any roles or responsibilities not contained in this document are either not provided with the Service Offering or assumed to be your responsibility.

VMware's service level commitments are set forth in in the Horizon Cloud Service with Microsoft Azure Service Level Agreement document available at the following link:

https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/support/vmware-horizon-cloud-on-azure-service-level-agt.pdf

2.1 Service Support

VMware will provide support for the software components of the Service Offering that are both hosted in the cloud and downloaded to Microsoft Azure. This includes support for deployment, account and desktop/application availability, access to the Horizon Cloud Manager, and selected additional services to assist with adoption of and related to the Service Offering. VMware will only provide support for Service Offering workloads.

Support will be provided by VMware's Global Support team pursuant to its standard procedures. Support may be provided by both US and non-US persons, as appropriate to meet VMware's support obligations. Support for infrastructure components on Microsoft Azure and your own premises, such as a File Server, Directory Service, DNS, and NTP, is not included.

Additional support information can be found at:

- SaaS Production Support Web Page:
  https://www.vmware.com/support/services/saas-production.html
- SaaS Support Policies:
  https://www.vmware.com/support/policies/saas-support.html

2.2 SERVICE PROVISIONING

VMware will be responsible for the following:

- Hosting, maintaining, and operating the VMware cloud control plane and the Horizon Cloud Manager, keeping it up to date with the latest software version.
- Providing the necessary software for setting up one or more Horizon Cloud Nodes in your Microsoft Azure capacity, and Node pairing with the cloud control plane.
- Enabling a secure https connection that is initiated from the Horizon Cloud Node to the cloud control plane.
- Providing software that is downloaded to the Horizon Cloud Node from the cloud control plane.
- Optional deployment of the Unified Access Gateway on your Microsoft Azure capacity to enable either remote or internal end-user access.
- Confirming the total number of seats purchased.
- Providing access to product documentation.

You will be responsible for the following:

- Sizing your Microsoft Azure infrastructure capacity and Service Offering capacity according to the number of users and workloads expected and maintaining the required Microsoft Azure infrastructure limits. The Microsoft Azure capacity must also include room for the necessary Horizon Cloud components:
  - Bootstrap (short-lived)
  - Horizon Cloud “Smartnode”
  - [Optional] Unified Access Gateway
  - [Optional] VMware Identity Manager Connector(s)
  - [Optional] RDS License Server(s) that may be installed in your Microsoft Azure capacity or in your on-premises environment
- Preparing the Microsoft Azure network as required, and optional connectivity to your on-premises network
- Providing network 443 access, and opening network ports for optional remote access via Unified Access Gateway
- Providing Active Directory that may be on-premises, running in Microsoft Azure VM, or replicated in Microsoft Azure, along with and completing Active Directory domain binding
- Creating the master image/gold pattern with licensed applications that you wish to publish

- Providing a file server and the requisite number of file shares suitable for use for storing the UEM configuration and settings
- Ensuring that you have the requisite valid Windows Server license, and or RDS CAL
- Windows Client OS licensing (if applicable, and if so, compliance with applicable license agreements)

2.3 DISASTER AVOIDANCE AND DISASTER RECOVERY

VMware will provide the following services with respect to disaster avoidance and disaster recovery:

- Routine backups of Service Offering cloud service components, which include customer accounts, license key and user license counts.

You are responsible for any item that is not listed as a responsibility of VMware. This includes but is not limited to the following:

- Data protection, such as routine backups of the data and content accessed or stored on Horizon Cloud on Microsoft Azure VMs or storage devices, end user data, desktop and application assignments, configuration settings, etc.

2.4 MONITORING

VMware will provide the following services with respect to monitoring:

Platform Monitoring:

- Monitoring the Service Offering cloud control plane infrastructure, top-layer management, user management interfaces, and performance of the Horizon Cloud Manager. VMware will provide a summary view of desktops that are provisioned and in use, in addition to the desktop quota utilization. VMware will not proactively monitor the software on the Horizon Cloud Node.

User Workload Monitoring:

- VMware will be able to monitor the user workloads and user access over an historic period of time. An option is provided in the Service Offering to disable this if desired.

You are responsible for the following services with respect to Monitoring:

- Monitoring the Microsoft Azure resource (CPU, memory, disk) utilization and available capacity of the Horizon Cloud Node with respect to the configured Horizon Cloud on Microsoft Azure workloads and Microsoft Azure limits.
- Monitoring the availability and performance of end user access to desktops and applications.
- Monitoring guest operating systems, deployment of applications, and end user behavior.

2.5 INCIDENT AND PROBLEM MANAGEMENT

VMware will provide incident and problem management services (e.g., severity classification, recording, escalation, and return to service) pertaining to:

- Infrastructure over which VMware has direct administrative and/or physical access and control, such as Horizon Cloud on Microsoft Azure cloud control plane servers, storage, and network devices.
- Service Offering software over which VMware has customer-provided administrative access and control, such as the Horizon Cloud Manager. This includes Service Offering software components that reside on the Horizon Cloud Node.

You are responsible for incident and problem management (e.g., detection, severity classification, recording, escalation, and return to service) pertaining to:

- Your account settings under our administrative management (domain, two-factor authentication).
- User-deployed and configured assets such as VMs, custom developed or third-party applications, custom or user-deployed operating systems, network configuration settings, and user accounts.
- Operating system administration, including the operating system itself or any features or components contained within it.
- Performance of user-deployed VMs, custom or third-party applications, your databases, and operating systems imported or customized by you, or other assets deployed and administered by you that are unrelated to the Horizon Cloud Manager or the Service Offering.
- Your Active Directory, DNS and other networking infrastructure.
- Microsoft KMS licensing infrastructure.
- On-premises file servers that are connected to the Horizon Cloud Node.
- Infrastructure performance of Horizon Cloud Node.
- Anything else not under the direct control and administration of VMware.

2.6 Change Management

VMware will provide the following change management elements:

- Processes and procedures to maintain the health and availability of the Horizon Cloud Manager or Service Offering components.
- Processes and procedures to release new code versions, hot fixes, and service packs related to the Horizon Cloud Manager and the Service Offering components, both in the cloud and on Microsoft Azure, for the health and stability of virtual desktops and applications.
- For software components that are downloaded to the Horizon Cloud Node, you can schedule an update via the Horizon Cloud Manager.

Scheduled maintenance and incident management may impact all workloads running on the Horizon Cloud Node. It is advisable to run only Service Offering workloads on the Horizon Cloud Node.

You are responsible for:

- Scheduling a time for the automatic updates of the Horizon Cloud Node:
  - You will have up to 90 days from the notice date to update the software versions; after 90 days, an update will automatically be scheduled if you have not performed the update.
- Management of changes to your VMs, operating systems, custom or third-party applications, and administration of general network changes within your control.
- Ongoing management of assignments, entitlements, and system configuration.
- Ongoing management and patching of Master Images and applications with the latest updates as required by your organization.
- Administration of self-service features provided through the VMware and Horizon Cloud Manager consoles, up to the highest permission levels granted to you. This includes but is not limited to VM and domain functions, backup administration, and general account management, etc.
- Cooperating with us when planned and emergency maintenance is required.

2.7 SECURITY

The end-to-end security of the Service Offering is shared between VMware and you. VMware will provide security for the aspects of the Service Offering over which we have sole physical, logical, and administrative level control. You are responsible for the aspects of the Service Offering over which you have administrative level access or control. The primary areas of responsibility between VMware and you are outlined below.

VMware will use commercially reasonable efforts to provide:

- **Physical Security:** Working with our service providers to protect the data centers housing the VMware cloud control plane from physical security breaches.
- **Information Security:** Protection of the information systems used to deliver the Service Offering over which we have sole administrative level control.
- **Network Security:** Protection of the networks containing our information systems up to the point where you have some control, permission, or access to modify your networks.
- **Security Monitoring:** VMware will monitor for security events involving the underlying cloud infrastructure servers, storage, networks, and information systems used in the delivery of the Service Offering over which we have sole administrative level control. This responsibility stops at any point where you have some control, permission, or access to modify an aspect of the Service Offering.
- **Patching and Vulnerability Management:** VMware will maintain the systems it uses to deliver the Service Offering, including the application of patches we deem critical for the target systems. VMware will perform routine vulnerability scans to surface critical risk areas for the systems we use to deliver the Service Offering. Critical vulnerabilities will be addressed in a timely manner.

You must address:

- **Information Security:** You are responsible for ensuring adequate protection of the information systems, data, content, or applications that you deploy and/or access on the Service Offering. This includes but is not limited to any level of patching, security fixes, data encryption, access controls, roles and permissions granted to your internal, external, or third-party users, etc.
- **Network Security:** You are responsible for the security of the networks over which you have administrative level control. This includes but is not limited to maintaining effective firewall rules, exposing only communication ports that are necessary to conduct business, locking down promiscuous access, etc. You are responsible for creating the Azure service principal and updating the key pairs by recycling them as appropriate.
- **Security Monitoring:** You are responsible for the detection, classification, and remediation of all security events that are isolated within your Service Offering account, associated with VMs, operating systems, applications, data or content surfaced through vulnerability scanning tools, or required for a compliance or certification program in which you are required to participate and which are not serviced under another VMware security program.

2.8 Data Access

In the event of issues that require diagnosis and troubleshooting, select personnel from the VMware Horizon Cloud operations team will have the ability to remotely log in to the Horizon Cloud Node appliances in your Microsoft Azure infrastructure to review and gather logs or to perform remote emergency remediation.

- VMware will be able to:
  - Obtain log files and crash reports from the Horizon Cloud Node, 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
- In addition, VMware will be able to collect product usage pattern, behavior and metrics anonymously on a regular basis to improve VMware products and services, fix problems, and provide recommendations for best practices. An option is provided in the Service Offering to disable this if desired.
- VMware will be storing information that includes customer contact information (name, email), Horizon Cloud Node data such as location, and audit information that covers life cycle events such as pairing with the cloud control plane, requests to download software etc.
- Transmission of the files from the Horizon Cloud Node to the cloud is done over an SSL channel but the files themselves are not encrypted at rest.

3. Business Operations

This section summarizes processes for ordering, scaling, renewing, suspending, and terminating the Service Offering.

3.1 Ordering and Invoicing

Subscription Ordering

- Initial orders for a core subscription for a single Service Offering instance ("Service Identifier" or SID) are described in Appendix A. Your initial purchase establishes the default billing relationship that applies to all transactions for that SID for the duration of the Subscription Term. For example, if the initial order is placed through a VMware authorized reseller, then, by default, any subsequent payments related to that Service Identifier will be made through that reseller. This billing relationship may be modified at renewal.
- The Subscription Term and the applicable billing period will begin within 24 hours of the date the Service Offering has been provisioned. VMware can elect to delay the start of the billing period at its discretion.
- There is an option to purchase either a Named User or a Concurrent User subscription, but a single order can only be for Named Users or Concurrent Users.
- Additional seats may be purchased at the time of your initial order or any time after the initial order. The additional capacity must be of the same type as the initial core subscription.
- You can order additional capacity (seats) any time before the end of the Subscription Term.
- Changes to the VMware authorized reseller associated with a SID may be made at the time of renewal by contacting VMware.

Invoicing

- If you purchase the Service Offering directly from VMware, VMware will invoice you within thirty (30) business days after the beginning of each Billing Period. If you purchase the Service Offering through a VMware authorized reseller, the reseller will invoice you as mutually agreed between you and such reseller. "Billing Period" is the period for which you are being billed for use of the Service Offering. Billing Periods are monthly and are related to the provisioning of your SID, unless otherwise indicated.

- You will be invoiced for the quantity of seats purchased regardless of whether the Service Offering is used or not.

3.3 Additional Capacity

Additional seats can be purchased in increments of 10 seats with the same licensing options. The Subscription Term for these additional seats will be coterminous with the initial core subscription

If add-on capacity causes you to achieve a higher volume tier (if applicable), any per-unit price reductions will apply to the remaining term of the SID if billed monthly. Prepaid subscriptions will not receive a refund for any per-unit price reduction due to achieving a higher volume tier. Per-unit price reductions will apply to add-on capacity for both monthly and prepaid subscriptions added after the higher volume tier is achieved.

3.4 Renewal

Renewal options for a SID may be selected using the My VMware administrative portal. Renewal options include:

Auto-Renewal (the default setting)

Except as set forth in this Section 3.4, each SID will automatically renew using the current configuration and the existing Subscription Term length. The then-current SKUs and pricing, based on the applicable price list, will be applied to the renewal term. You may opt out of auto-renewal by changing your renewal option setting for the SID within the My VMware Portal available at http://my.vmware.com. The deadline to change the renewal option is 30 days prior to the last day of the SID's current Subscription Term.

Modify Subscription Service at End of Term

When this option is selected, you may be contacted prior to the end of the Subscription Term to discuss your renewal options. You may modify your Service Offering configuration and make changes to your reseller relationship, if applicable, by both changing your setting for the SID within the My VMware Portal available at http://my.vmware.com and issuing a new purchase order. If you do not make any changes to your current SID by the deadline below and/or you do not issue a new purchase order to VMware or to your VMware authorized reseller, your existing SID, as currently configured, will automatically renew. If you purchase the Service Offering through a VMware authorized reseller, a manual renewal is the only time you may change your reseller relationship for that specific SID. The deadline to change the renewal option is 30 days prior to the last day of the SID's current Subscription Term.

Terminate at End of Term

You may terminate your existing SID renewal by changing your setting for the SID within the My VMware Portal available at http://my.vmware.com. When this option is set, then your access to the Service Offering will expire at the end of the SID's then-current Subscription Term. The deadline to select this termination option is 30 days prior to the last day of the SID's current Subscription Term.

VMware reserves the right to not renew a SID at the end of its Subscription Term. In the event of a non-renewal by VMware, we will notify you 30 days prior to the end of the Subscription Term.

3.5 Suspension and Re-Enablement

While a SID is suspended by VMware for delinquent payment or any other reason as detailed in the Terms of Service, VMware will restrict access to Horizon Cloud Manager for subsequent orchestration. VMware will retain SIDs with configurations and data intact until the issue is resolved or your Subscription Term expires or is terminated.

SID re-enablement will be initiated promptly upon resolution of the account issues that led to suspension; access to the Service Offering and traffic across IP addresses will be restored.

3.6 TERMINATION

Full termination of a SID due to expiration, termination, cancellation, or any other cause will result in loss of access to Horizon Cloud Manager, discontinuation of software updates, account services, and support.

Data from a terminated SID will not be retained by VMware beyond the termination date of such SID.

Appendix A – Horizon Cloud

Horizon Cloud on Microsoft Azure	
Horizon Cloud on Microsoft Azure software	Virtualized application and desktop delivery with RDS-hosted applications and desktops published on BYO Microsoft Azure infrastructure capacity
Horizon Cloud Manager cloud access	VMware Cloud-hosted management
Horizon Client	Application that allows end users to connect to the virtual desktop from client end points
Unified Access Gateway	Optional virtual appliance that allows secure remote access to end user computing resources by authorized users connecting either externally and/or internally
DaaS Agent	Set of agents that are installed on all the virtual desktops to communicate with the back-end platform
Horizon Agent	
User Environment Agents	
User Environment Manager	Stand-alone console for User Environment Manager
VMware Identity Manager	Optional service that allows for single sign-on (SSO) for Horizon Cloud apps and desktops, ensure security with multi-factor authentication and control conditional access

APPENDIX B - HORIZON CLOUD GUEST OS COMPATIBILITY TABLE

Horizon Cloud on Microsoft Azure supports the use of the following Windows operating systems on virtual machines hosted within the Horizon Cloud on Microsoft Azure Appliance

Operating System	Patch / SP	32 / 64 bit	Additional Variants / Specs	VDI / RDSH
Windows 10	See knowledge base link below for latest version support	64		VDI
Windows Server 2012 R2		64		RDSH
Windows Server 2016		64		RDSH

Supported languages are English and Japanese. Supported language packs are French, French Canadian, and German.

For supported build versions of Microsoft Windows 10, see: https://kb.vmware.com/s/article/53182

APPENDIX C – MICROSOFT LICENSING RECOMMENDATIONS

The following are recommendations only. You must verify licensing requirements and restrictions with your Microsoft Licensing distributor.

Horizon Cloud on Microsoft Azure does not provide any guest OS licensing required for the full use of the Horizon Cloud on Microsoft Azure solution. All necessary Microsoft licenses for operating Desktops and Microsoft Applications are available from your preferred Microsoft Licensing distributor.