Service Description

VMware Horizon® Service

Updated as of: 06 April 2020

vmware®

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.

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

Table of Contents

1. INTRODUCTION

VMware Horizon® Service ("Horizon Service" or the "Service Offering") includes three individual services: VMware Horizon® 7 subscription, VMware Horizon® Cloud Service™ on Microsoft Azure, and VMware Horizon® Cloud Service™ on IBM Cloud.

- Horizon 7 subscription delivers virtual desktops and applications on either a customer's own on-premises infrastructure or on the customer's VMware Cloud™ on AWS infrastructure, and connects to the Horizon Cloud control plane through the VMware Horizon® 7 Cloud Connector™.
- Horizon Cloud Service on Microsoft Azure delivers cloud-hosted virtualized desktops and applications from a customer's own Microsoft Azure infrastructure capacity. Customers pair their Microsoft Azure infrastructure capacity with this service.
- Horizon Cloud Service on IBM Cloud delivers cloud-hosted virtualized desktops and applications from a VMware-managed environment on IBM Cloud. In order to use Horizon Cloud Service on IBM Cloud, customers must also purchase IBM Cloud capacity.

The Service Offering provides access to the Horizon Cloud control plane, that is hosted by VMware in third-party data centers located in the United States of America, Germany, and Australia. The Horizon Cloud control plane provides access to the VMware Horizon® Cloud Manager™ console to orchestrate and manage the customer's Horizon Service workloads. The status of the Horizon Cloud control plane, and the IBM Cloud data centers where the Horizon Cloud Service on IBM Cloud is hosted, can be viewed at: https://status.horizon.vmware.com.

1.1 HORIZON SERVICE - CAPABILITIES

The Service Offering includes the following capabilities:

- **Domain Binding** via Horizon Cloud Manager, to set up active directory, administrator roles and permissions, and end user groups.
- **Unified Dashboard** via Horizon Cloud Manager, that provides a single pane of glass overview into health status and connectivity metrics of the Horizon Pods.
- **Capacity Page** via Horizon Cloud Manager, that provides a single pane of glass overview into the resource utilization of the Horizon Pods.
- **Helpdesk** via Horizon Cloud Manager, to enable support teams and administrators to get detailed session insight and troubleshoot Horizon deployments.
- **Automated Installation of Horizon 7 subscription on VMware Cloud on AWS** via Horizon Cloud Manager, to reduce deployment time and automatically create a cloud-connected Horizon Pod.
- **Integration with User Customization** that allows the customer to customize its end user environments. This can be enabled through a separate VMware Dynamic Environment Manager™ console.
- **Optional VMware Workspace ONE®** integration via VMware Workspace ONE® Access™, which provides end users with identity-based catalog access to their assigned desktops and applications.

If a particular service, feature, or functionality of the Horizon Service is not expressly provided or specified in this Service Description or elsewhere in the Agreement, then it is not available, and VMware is under no obligation to provide such service, feature, or functionality.

1.2 MICROSOFT WINDOWS OS LICENSING AND SUPPORT

For all virtual machine Microsoft OS licensing (Windows client or server OS), customers must use their own licenses purchased through their Microsoft licensing distributor. Customers are required to initiate all in-guest troubleshooting through the Microsoft support process. See Appendices C, D, E and F for details on supported Guest OS and Microsoft licensing guidance.

1.3 End User Access to Desktops and Applications

Desktops and applications can be accessed via VMware Horizon® Client™ or via VMware Horizon® HTML Access™. Use of these offerings is governed by the standard VMware end user license agreement ("EULA") which incorporates the VMware Product Guide, copies of which are available through the links at the main VMware terms landing page, found at http://www.vmware.com/download/eula. If there is a conflict between the EULA and the Agreement (as defined in the Terms of Service), the terms of the Agreement will govern.

1.4 Workspace ONE Access

The Service Offering includes Workspace ONE Access, hosted by VMware. With Workspace ONE Access, you can set up single sign-on (SSO) for VMware Horizon® desktops and applications, support security with multi-factor authentication (including VMware Workspace ONE® Verify, VMware's multi-factor authentication solution included in Workspace ONE Access that is powered by a third-party service provider), and control conditional access. If you 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 in connection with your use of Workspace ONE Verify. 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 in any other country in which VMware or its affiliates or service providers maintain facilities.

Use of Workspace ONE Access within the Service Offering requires a Workspace ONE Access connector, which can be installed and managed on a customer's virtual machine or on a utility server in Horizon Cloud on IBM Cloud (Standard Desktop Capacity ("SDC") cost is determined based on server sizes required).

Workspace ONE Access may only be used for SSO, identity federation, multi-factor authentication, and app catalog access for your Service Offering desktops and applications. If you want to use Workspace ONE Access with any application not delivered by the Service Offering, consult your VMWare sales representative to purchase the appropriate Workspace ONE Access entitlement.

1.5 Additional Information and Legal Terms

General Definitions

For purposes of this Service Description:

"Active Connection" means (i) with respect to VMware Horizon® View™ (for Microsoft Windows), VMware Dynamic Environment Manager™, and VMware Horizon® for Linux, any connections to Powered On Desktop Virtual Machines, Terminal Services Sessions and physical computers, and (ii) with respect to VMware Mirage™, any provisioned desktop image.

"Bandwidth" in regard to VMware Horizon Cloud Service on IBM Cloud is the network connectivity from your VMware Horizon Cloud Service on IBM Cloud environment to the public Internet using VMware's Internet service providers. Bandwidth is consumed when data is either transferred or received by your purchased class of service.

"Concurrent Users" means the total number of users accessing or using the Service Offering at any given time to maintain an Active Connection, including active and idle session states, to their workspace or desktop through each endpoint device. For purposes of this Service Description, an "endpoint" device includes, but is not limited to, laptops, desktops, tablets, and similar hardware.

"Dedicated Desktop" is a desktop that retains, from one session to another, user entitlements to that desktop as well as any changes done to that desktop's operating environment by the user.

"Desktop Model" in regard to VMware Horizon Cloud Service on IBM Cloud is a bundle of compute, memory, storage, and bandwidth capacity that consists of a multiple of Standard Desktop Capacity and that can be instantiated as a desktop. For example, a desktop model may have twice as much resources as a Standard Desktop Capacity.

"Desktop Virtual Machine" is a hosted Virtual Machine with one of the following Microsoft Windows operating systems: 7, 8, 10, or Server.

"Device" as used in this Service Description means any client hardware that enables installing and running any of the modalities of the Service Offering on that client hardware.

"Floating Desktop" is a desktop that does not retain any changes from one session to another.

"vGPU" is the ability to use a physical graphics processing unit ("GPU") installed on a server to create virtual GPUs that can be shared across multiple virtual machines.

"High Availability" in regard to VMware Horizon Cloud Service on IBM Cloud, refers to the ability to restart a provisioned workload on a different server in the cluster, if the workload's current server fails to function properly, to allow users to access their workload in the event of a single server failure. Some data loss may occur during this transition from one server to another in the cluster.

"Horizon Pod" is the VMware software that is deployed into the supported infrastructure capacity.

"Image Templates" in regard to VMware Horizon Cloud Service on IBM Cloud, are master images that can be modified in the administration console and that are used to create virtual desktops.

"IOPS" (pronounced "eye-ops") means input/output operations per second, and is a performance measurement used to characterize computer storage devices like hard disk drives (HDD), solid state drives (SSD), and storage area networks (SAN).

"IP Addresses" are used to provide connectivity from the public Internet.

"LUN" in computer storage, is a logical unit number used to identify a logical unit, which is a device addressed by the SCSI protocol or storage area network protocols which encapsulate SCSI, such as Fiber Channel or iSCSI.

"Named User" means your employee, contractor, or Third-Party Agent who has been specifically authorized by you (i.e., by name) to use the Service Offering in accordance with the Agreement.

"NAT" is a method of remapping one IP address space into another by modifying network address information in Internet Protocol (IP) datagram packet headers while they are in transit across a traffic routing device.

"Plan Charges" are charges for those Service Offering components that you have committed to purchase and are recurring during the Subscription Term without regard to usage. These charges will be invoiced for the then-current Billing Period as described in Section 5.1 of this Service Description.

"Seat" as used in this Service Description, can be either a Named User or a Concurrent User, as applicable for the particular service.

"Standard Desktop Capacity" (or "**SDC**") in regard to VMware Horizon Cloud Service on IBM Cloud, is a fixed bundle of compute, memory, storage, and bandwidth capacity that can be instantiated as a desktop.

"Storage" in regard to VMware Horizon Cloud Service on IBM Cloud, contains block level VM capacity surfaced to you through your purchased class of service. Storage is ordered in defined increments. Storage usage is intended for core operating system and applications only.

"Terminal Services" (known as Remote Desktop Services (RDS) in Windows Server 2012 and later) is a component of Microsoft Windows that allows a user to take control of a remote computer or virtual machine over a network connection.

"Third-Party Agent" means a third party delivering information technology services to you pursuant to a contract with you.

"**VDI**" (or Virtual Desktop Infrastructure) is the technology for providing and managing virtual desktops.

"Virtual Machine" or "**VM**" means a software container that can run its own operating system and execute applications like a physical machine.

Other terms used but not defined in this Service Description have the meanings set forth in the standard VMware Cloud Service Offerings Terms of Service ("Terms of Service"), or elsewhere in the Agreement (as defined in the

Terms of Service), or in the standard VMware End User License agreement ("EULA"), and the associated Product Guide, all of which are available through links on the main VMware end user terms landing page, located at https://www.vmware.com/download/eula.html.

Technical Documentation and Training

Online help outlining Key Concepts with usage examples, a "Deployment Guide", and a "Administration Guide" is available at https://docs.vmware.com/en/VMware-Horizon-Cloud-Service/index.html

Legal Terms

Unless otherwise specified, hosted elements of the Service Offering are subject to the Terms of Service, and on-premise elements of the Service Offering are subject to the EULA and the Product Guide, all of which are available through links on the main VMware end user terms landing page, located at https://www.vmware.com/download/eula.html. If there is a conflict between the EULA and the Agreement (as defined in the Terms of Service), the terms of the Agreement will govern.

Usage Data

The Service Offering collects data directly from the machines and/or devices involved in the use of the Service Offering, such as configuration, performance, and usage data, for the purposes of improving VMware products and services, and your and your users' experiences, as more specifically described in VMware's Trust and Assurance Center, found at https://www.vmware.com/solutions/trustvmware/usage-data-programs.html. To the extent that any of this data is considered personal data under applicable data protection laws, the data will be treated in accordance with the VMware Privacy Notice, found at https://www.vmware.com/help/privacy.html. In connection with the collection of usage data, VMware and its service providers use cookies. Detailed descriptions of the types of cookies we use can be found in the VMware Privacy Notice referenced above, and policies linked from that Privacy Notice. More information on how to choose whether to accept certain cookies used by VMware websites and solutions can also be found from that link.

2. VMware Horizon 7 Subscription

VMware Horizon 7 subscription includes (i) software installed in your own infrastructure (whether in your on-premise environment or in your VMware Cloud™ on AWS environment) that allows deployment and use of virtual desktops and of applications, and (ii) access to the hosted Horizon Cloud control plane via the Horizon Cloud Manager management console, to orchestrate and manage your Horizon Service workloads.

To use the Horizon 7 subscription offering, you must provide your own infrastructure capacity, whether that capacity is in your own on-premise environment or in your VMware Cloud on AWS environment. You can either (i) connect an existing, already deployed VMware Horizon 7 environment, whether in your on-premise environment or in your VMware Cloud on AWS instance, to the Horizon Cloud control plane, or (ii) use the Horizon Service to automatically install Horizon 7 subscription in your VMware Cloud on AWS environment.

To connect an existing Horizon 7 environment (whether in your on-premise environment or in your VMware Cloud on AWS environment) to the Horizon Cloud control plane, you must deploy the Horizon 7 Cloud Connector, which is a virtual appliance that pairs with the Horizon Cloud control plane and creates an appropriately configured cloud-connected "Horizon Pod" (or "Pod").

If you use the Horizon Service to automatically install the Horizon 7 subscription service into your VMware Cloud on AWS environment, installation includes deployment of the Horizon Cloud Connector and pairing with the Horizon Cloud control plane, creating a cloud-connected Horizon Pod. After installation into your VMware Cloud on AWS environment is complete, you will be responsible for continuing to build out the environment as needed. Once the pairing is complete, you can use the Horizon Cloud Manager to manage the Horizon 7 subscription environment along with the on-premise Horizon Console (i.e., the main console used to manage the on-premise Horizon VDI environment).

Regardless of the method you use to deploy the Horizon 7 subscription service, you are responsible for managing your Horizon 7 subscription environment.

2.1 HORIZON 7 SUBSCRIPTION SERVICE CAPABILITIES

The Horizon 7 subscription service includes the following capabilities:

- **Pairing** of the Horizon 7 subscription infrastructure with the Horizon Cloud control plane through the Horizon Cloud Connector and subsequent configuration of the supported capabilities.
- **Windows Desktops** allows for delivery of virtual desktops (or virtual desktop infrastructure, "VDI") based on the Windows operating system.
- **Linux Desktops** allows for delivery of virtual desktops based on the Linux operating system.
- **RDSH-Published Applications and Session-Based Desktops** allows for the delivery of the published applications and session-based desktops running on RDSH servers.
- **App Volumes** allows for application delivery to both virtual desktops and RDSH servers.
- **Session Collaboration** allows users to invite other users to join an existing Windows remote desktop.
- **Cloud Monitoring** is used to capture and display guest VM performance and usage statistics.

2.2 HORIZON 7 SUBSCRIPTION SERVICE PORTALS

The Horizon 7 subscription service includes access to two self-service consoles:

- **My VMware Account Management Console** provides access to your Horizon 7 subscription status, integrating navigation, viewing, and management of all VMware product entitlements and support under a single account. It also allows download of the Horizon 7 subscription software components.
- **VMware Horizon Cloud Manager Console** is the primary interface for consumption and management for the Horizon 7 subscription service, including domain binding, gold pattern management, desktop provisioning, application provisioning, user customization provisioning, end user entitlement, and other management operations.

2.3 HORIZON 7 SUBSCRIPTION SERVICE OPERATIONS

The following outlines VMware's roles and responsibilities in delivery of the Horizon 7 subscription service. While specific roles and responsibilities have also been identified as being owned by you, any roles or responsibilities not contained in this Service Description are either not provided with the Horizon 7 subscription service or are assumed to be your responsibility.

2.3.1 HORIZON 7 SUBSCRIPTION - SUPPORT

VMware will provide support for problems that you report and selected additional support services to assist with adoption of and related to the Horizon 7 subscription service. VMware will only provide support for Horizon 7 subscription workloads. Support may be provided in any country in which VMware or its providers maintain facilities. If you provide Content (as defined in the Terms of Service) in connection with support requests, VMware will handle that Content in accordance with the Terms of Service. Support for customer-controlled infrastructure components on VMware Cloud on AWS and in your own on-premise infrastructure, such as a File Server, Directory Service, DNS, and NTP, is not included with the Horizon 7 subscription service.

Supported versions of the Horizon 7 subscription service include the latest three production release versions. Customers on older versions will not be eligible for support and are encouraged to keep up with VMware change management requests.

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

2.3.2 HORIZON 7 SUBSCRIPTION - PROVISIONING

VMware will be responsible for the following:

- Hosting, maintaining, and operating the Horizon Cloud control plane and Horizon Cloud Manager.
- Confirming the total number of user entitlements purchased.
- Providing access to product documentation.
- Providing the necessary software for setting up one or more Horizon Pods in your on-premise environment or in your VMware Cloud on AWS environment.
- Enabling a secure https connection that is initiated from the Horizon Cloud Connector to the Horizon Cloud control plane.

You will be responsible for the following:

- Ensuring that you have the requisite valid Windows Server license, and or RDS CAL (if applicable, and, if so, compliance with applicable license agreements).
- Windows Client OS licensing (if applicable, and if so, compliance with applicable license agreements).
- Providing Active Directory and completing Active Directory domain binding.
- Deployment and configuration of VMware Dynamic Environment Manager.
- Deployment and configuration of the Workspace ONE Access connector and configuration of Workspace ONE Access.
- Deploying the VMware Horizon Cloud Connector and pairing it to the Horizon Cloud control plane.
- Deploying and building out, as needed, the Horizon 7 subscription environment, whether in your on-premise infrastructure or in your VMware Cloud on AWS environment, unless the Horizon Service is used to automatically deploy a Horizon Pod into your VMware Cloud on AWS environment.
- Continuing to build out the Horizon 7 subscription environment as needed if using the Horizon Service to automatically deploy a Horizon Pod into your VMware Cloud on AWS environment.
- Managing the Horizon 7 subscription environment, whether in your on-premise infrastructure or in your VMware Cloud on AWS environment.

2.3.3 HORIZON 7 SUBSCRIPTION - DISASTER AVOIDANCE AND DISASTER RECOVERY

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

- Data protection, such as routine backups of the hosted service components, which include accounts, license keys, entitlement and license counts, top-layer management and user-management interfaces owned and operated by VMware.
- Data and infrastructure restoration of the hosted service components, including management and user-management interfaces owned and operated by VMware.

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 7 subscription VMs or storage devices, end user data, desktop and application assignments, configuration settings, etc.
- NOTE: VMware does not provide backup or recovery for any customer-managed assets such as customer-provisioned VMs and Images.

2.3.4 HORIZON 7 SUBSCRIPTION - MONITORING

VMware will provide the following services with respect to monitoring:

Platform monitoring:

- Monitoring the Horizon Cloud control plane infrastructure, top-layer management, user-management interfaces, and performance of the Horizon Cloud Manager.
- Horizon Cloud control plane status can be viewed at: http://status.horizon.vmware.com/

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

- Monitoring the availability and performance of end user access to desktops and applications.
- Monitoring guest operating systems and applications inside the guest storage utilization, and end user behavior.
- Monitoring dedicated network connectivity / VPN, or application vulnerabilities.
- Monitoring the assets deployed within your own infrastructure (whether hosted or on-premise) that are critical to the Horizon 7 subscription service, including but not limited to Domain Controller, Active Directory, DHCP, VPN, and user roles and permissions.

2.3.5 HORIZON 7 SUBSCRIPTION - 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 the Horizon Cloud control plane servers, storage, and network devices.
- Those portions of the Horizon 7 subscription environment over which VMware has customer-provided administrative access and control, such as the Horizon Cloud Manager.

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 even if the source is supplied from VMware. For any operating system issues, please contact your operating system support organization.
- 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 Horizon 7 subscription service.
- Your Active Directory, DNS, and other networking infrastructure including VPN integration.
- Microsoft KMS licensing infrastructure.

- Infrastructure performance of any Horizon Pod
- Anything else not under the direct control and administration of VMware.

2.3.6 HORIZON 7 SUBSCRIPTION - 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 Horizon 7 subscription service components.
- Processes and procedures to release new code versions, hot fixes, and service packs related to Horizon 7 subscription service components to maintain the health and stability of virtual desktops and applications.

You are responsible for:

- 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 Horizon Cloud Manager console, 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.

2.3.7 HORIZON 7 SUBSCRIPTION - SECURITY

The end-to-end security of the Horizon 7 subscription service is shared between VMware and you. VMware will provide security for the aspects of the Horizon 7 subscription service over which we have sole physical, logical, and administrative level control. You are responsible for the aspects of the Horizon 7 subscription service 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 hosted portions of the Horizon 7 subscription service from physical security breaches.
- **Information Security:** Protection of the information systems used to deliver the Horizon 7 subscription service 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 Horizon 7 subscription service 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 Horizon 7 subscription service.
- **Patching and Vulnerability Management:** VMware will maintain the systems we use to deliver the Horizon 7 subscription service, including applying 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 hosted portions of the Horizon 7 subscription service. 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 Horizon 7 subscription service. 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.
- **Security Monitoring:** You are responsible for the detection, classification, and remediation of all security events that are isolated within your Horizon 7 subscription service 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.

3. VMware Horizon® Cloud Service™ on Microsoft Azure

Horizon Cloud Service on Microsoft Azure includes (i) software that allows the deployment and use of desktops and applications hosted on your Microsoft Azure infrastructure capacity, and (ii) access to the Horizon Cloud control plane via the Horizon Cloud Manager management console, to orchestrate and manage your virtual workloads.

For the Horizon Cloud Service on Microsoft Azure service, you must provide your own Microsoft Azure subscription. During onboarding, the software required to use the Horizon Cloud Service on Microsoft Azure service is automatically deployed into your Microsoft Azure environment. The deployed software creates a Horizon Pod, which pairs with the Horizon Cloud control plane. After the Horizon Pod 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 your Microsoft Azure 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 Microsoft Azure capacity at the same time.

Horizon Cloud Service on Microsoft Azure supports the majority of Microsoft Azure VM Sizes for either virtual desktops or Farms across Microsoft Azure’s global regions. Availability of the Microsoft Azure VM Sizes is dependent upon your Microsoft Azure subscription and availability of the VM Size in the specific Microsoft Azure region. VMware will at times remove VM Sizes from within your Horizon Cloud Service on Microsoft Azure instance that are not recommended for virtual desktops and/or Farms.

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 and/or Farms that can be hosted will vary on the VM instance type and the hardware resource capacity available within your current Microsoft Azure instance limits, up to a maximum of 2,000 concurrent connected sessions per Horizon Pod and 2,000 VMs per Microsoft Azure instance.

3.1 Horizon Cloud Service on Microsoft Azure Capabilities

Horizon Cloud Service on Microsoft Azure includes the following capabilities:

- **Pairing** of your Microsoft Azure infrastructure capacity with the Horizon Cloud control plane via the automatic build-out of the Horizon Cloud components on your Microsoft Azure infrastructure capacity and subsequent configuration through the Horizon Cloud Manager.
- **Desktop master image / gold pattern creation and management** through the ability of Horizon Cloud Service on Microsoft Azure 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 the 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 that users can access.
- **Power management** of your 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 Horizon Client, Horizon HTML Access, or Workspace ONE Access.
- **Cloud monitoring** is used to capture and display guest VM performance and usage statistics.

3.2 Horizon Cloud Service on Microsoft Azure - Service Portals

Horizon Cloud Service on Microsoft Azure includes access to three self-service consoles:

- **My VMware Account Management Console** provides access to subscription status, integrating navigation, viewing and management of all VMware product entitlements and support under a single account. It also allows download of the Horizon Service software components.
- **Horizon Cloud Manager Console** is the primary interface for consumption and management for Horizon Cloud Service on Microsoft Azure, including domain binding, gold pattern management, desktop provisioning, application provisioning, user customization provisioning, end user entitlement, and other management operations.
- **VMware Horizon® HTML Access™ Portal** is the primary web interface for end users accessing the desktop and published apps. This interface provides browser-based access via HTML5. Users are not required to use the portal to access their desktop or app – they can do so with the Horizon Client that is supported on Windows, Mac, Linux, iOS, Android, and through various third-party thin clients and zero clients.

3.3 Horizon Cloud Service on Microsoft Azure - Service Operations

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

3.3.1 Horizon Cloud Service on Microsoft Azure - Support

VMware will provide support for problems that you report and selected additional services to assist with adoption of and related to Horizon Cloud Service on Microsoft Azure. VMware will only provide support for workloads on this offering. Support may be provided in any country in which VMware or its providers maintain facilities. If you provide Content (as defined in the Terms of Service) in connection with support requests, VMware will handle that Content in accordance with the Terms of Service. Support for customer-controlled infrastructure components on Microsoft Azure or on your own premises, such as a File Server, Directory Service, DNS, and NTP, is not included.

For Horizon Cloud Service on Microsoft Azure, supported versions include the latest two production release versions. Customers on older versions will not be eligible for support and are encouraged to keep up with the VMware change management requests.

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

3.3.2 HORIZON CLOUD SERVICE ON MICROSOFT AZURE - PROVISIONING

VMware will be responsible for the following:

- Hosting, maintaining, and operating the Horizon Cloud control plane and Horizon Cloud Manager, keeping both up to date with the latest software versions.
- Providing the necessary software for setting up one or more Horizon Pods in your Microsoft Azure capacity, to allow the Horizon Pod pairing with the Horizon Cloud control plane.
- Enabling a secure https connection that is initiated from the Horizon Pod to the Horizon Cloud control plane.
- Providing software that is downloaded to the Horizon Pod from the Horizon Cloud control plane.
- Optional deployment of the VMware 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 Horizon Cloud Service on Microsoft Azure capacity according to the number of users and workloads expected, and maintaining the required Microsoft Azure infrastructure limits. Your Microsoft Azure capacity must also include room for the necessary Horizon Cloud components:
  - Jumpbox VM that is used during the deployment and upgrade of the Horizon Pod, and that is automatically deleted after the completion of a deployment or upgrade. The Jumpbox VM is also required by VMware in order to support Horizon Cloud Service on Microsoft Azure, and can be deployed as needed to support the service. It is deleted by VMware after completion of the support request.
  - Horizon Pod manager VM
  - Azure Database for PostgreSQL Service
  - [Optional] A second Horizon Pod manager VM if High Availability feature is enabled
  - [Optional] Unified Access Gateway VMs
  - [Optional] VMware Workspace ONE Access connector(s)
  - [Optional] RDS License Server(s) that may be installed in your Microsoft Azure capacity or in your on-premise environment
- Preparing the Microsoft Azure network as required, and optional connectivity to your on-premise network.
- Providing network 443 access, and opening network ports for optional remote access via Unified Access Gateway.
- Providing Active Directory, that may be on-premise, running in Microsoft Azure VM, or replicated in Microsoft Azure, 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 Dynamic Environment Manager 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).

3.3.3 HORIZON CLOUD SERVICE ON MICROSOFT AZURE - DISASTER AVOIDANCE AND DISASTER RECOVERY

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

- Data protection, such as routine backups of the service's hosted components, which include customer accounts, license keys, license counts, top-layer management and user-management interfaces owned and operated by VMware.
- Data and infrastructure restoration of the service's hosted components, including management and user-management interfaces owned and operated by VMware.

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.
- NOTE: VMware does not provide backup or recovery for any customer-managed assets such as customer-provisioned VMs and Images.

3.3.4 HORIZON CLOUD SERVICE ON MICROSOFT AZURE - MONITORING

VMware will provide the following services with respect to monitoring:

Platform Monitoring:

- Monitoring the Horizon Cloud control plane infrastructure, top-layer management, user-management interfaces, performance of the Horizon Cloud Manager.
- Horizon Cloud control plane status can be viewed at: http://status.horizon.vmware.com/

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 to disable this if desired.

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

- Monitoring your Microsoft Azure resource (CPU, memory, disk) utilization and available capacity of the Horizon Pod with respect to the configured Horizon Cloud on Microsoft Azure workloads and Microsoft Azure instance limits.
- Monitoring the availability and performance of end user access to desktops and applications.
- Monitoring guest operating systems, applications, inside the guest storage utilization and end user behavior.
- Monitoring dedicated network connectivity / VPN, or application vulnerabilities.
- Monitoring the assets deployed within your own corporate infrastructure (either on-premise or hosted by a third party) that are critical to Horizon Cloud Service on Microsoft Azure operations, including but not limited to Domain Controller, Active Directory, DHCP, VPN, and user roles and permissions.

3.3.5 HORIZON CLOUD SERVICE ON MICROSOFT AZURE - 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 the Horizon Cloud control plane servers, storage, and network devices.
- Elements of the service over which VMware has customer-provided administrative access and control, such as the Horizon Cloud Manager. This includes software components that reside on the Horizon Pod.

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 even if the source is supplied from VMware. For any operating system issues, contact your operating system support organization.
- 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.
- Your Active Directory, DNS and other networking infrastructure including VPN integration.
- Microsoft KMS licensing infrastructure.
- On-premise file servers that are connected to any Horizon Pod
- Infrastructure performance of any Horizon Pod
- Anything else not under the direct control and administration of VMware.

3.3.6 Horizon Cloud Service on Microsoft Azure - 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 components.
- Processes and procedures to release new code versions, hot fixes, and service packs related to the Horizon Cloud Manager and the service components for the health and stability of virtual desktops and applications.
- For software components that are downloaded into the Horizon Pod, you can schedule an update via the Horizon Cloud Manager.

You are responsible for:

- Scheduling a time for automatic updates of the software components running in the Horizon Pod:
  - You will have up to a maximum of 90 days from the notice date (shown in the admin console) to update the software versions in the Horizon Pod; 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 Horizon Cloud Manager console, 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 VMware when scheduled or emergency maintenance is required.
- "Scheduled maintenance" is defined as pre-scheduled maintenance that has the potential to impact availability of the customer's environment.
    - Maintenance windows: Scheduled maintenance is generally performed between the hours of 12:00AM (Midnight) to 6:00AM (local time) for the Microsoft Azure Regions in which the Horizon Pods are deployed. However, on rare occasions it may be necessary for VMware to perform maintenance outside of this window, and VMware reserves the right to do so.
    - Advance notice: A minimum of 24 hours advance notice will be given for scheduled maintenance.
- "Emergency maintenance" is defined as potentially impactful maintenance activity that must be executed quickly due to an immediate, material threat to the security, performance, or availability of the service. Every attempt will be made to provide as much advance notice as possible, but notice depends on the severity and critical nature of the emergency maintenance.

3.3.7 HORIZON CLOUD SERVICE ON MICROSOFT AZURE - SECURITY

The end-to-end security of the Horizon Cloud Service on Microsoft Azure is shared between VMware and you. VMware will provide security for the aspects of the service over which we have sole physical, logical, and administrative level control. You are responsible for the aspects of the service 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 service from physical security breaches.
- **Information Security:** Protection of the information systems used to deliver the service 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 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.
- **Patching and Vulnerability Management:** VMware will maintain the systems it uses to deliver the service, 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. 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. 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 Microsoft 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 environment, 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.

3.3.8 Horizon Cloud Service on Microsoft Azure - Data Access

In the event of issues that require diagnosis and troubleshooting, select personnel from the VMware Horizon Cloud Service operations team will have the ability to remotely log in to the Horizon Pod 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 Pod, which will show usernames, 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 Pod
  - Have real-time access to the current operational health status of the Horizon Pod
- 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 to disable this if desired.
- VMware will be storing information that includes customer contact information (name, email), Horizon Pod data such as location, and audit information that covers life cycle events such as pairing with the Horizon Cloud control plane, requests to download software, etc.
- Transmission of files from the Horizon Pod to the Horizon Cloud control plane is done over an SSL channel, but the files themselves are not encrypted at rest.

4. VMware Horizon® Cloud Service™ on IBM Cloud

Horizon Cloud Service on IBM Cloud has the following features:

- Horizon Cloud Service running on bare metal hosts deployed in the IBM Cloud.
- Tenant onboarding and change management service.
- Three distinct workload options: Horizon Cloud Desktops, Horizon Cloud Apps, and Horizon Cloud Graphical Workstations.
- Three different host types capable of running workloads with and without a virtual Graphics Processor Unit.
- Ten different VM types, from an efficient “Value Desktop” to the high-performance “M60 Performance” workstation.
- Maintenance, patching, and upgrades of the platform and the physical infrastructure performed by VMware.

4.1 Horizon Cloud Service on IBM Cloud - Options

An entitlement to the Horizon Cloud Service on IBM Cloud service consists of (i) a subscription to the service, and (ii) IBM Cloud capacity, on a per-host basis, that allows the customer to provision one or more workloads available on the type of capacity provisioned on that host.

Horizon Cloud Service on IBM Cloud provides the following host types:

Host type	Standard Host	vGPU Workstation (M60)
CPU	Dual Intel Xeon Gold 6248 (40 Cores, 2.50 GHz) x 2	Intel Xeon E5-2690 v4 (28 Cores, 2.60 GHz) x 2
RAM (GB)	384	512
Usable HD Storage (GB)	10,000	6,000
vGPU	N/A	NVIDIA Tesla M60 GPU Accelerator x 2

NOTE: VMware will have the right to substitute alternate host hardware, as newer configurations become available, so long as the customer receives at least the same capacity as under the hardware capacity configuration as originally ordered. As an example only, assume an existing server can host 120 SDCUs, and a customer bought an entitlement for 600 SDCUs (that is, five host servers, under the existing configuration). Assume also that, under the new host hardware specifications, each server can host 210 SDCUs. In that case, VMware can upgrade the customer to three host servers (rather than the previous five host servers), providing the same capacity.

For customers that want a short-term, low-cost proof of concept of the Horizon Cloud Service on IBM Cloud, a "Starter Edition" bundle is available, which includes both (i) a subscription to the service, and (ii) capacity on a single Standard Host, with month-to-month pricing (see details below)

Horizon Cloud Service on IBM Cloud - Capacity Types

IBM Cloud capacity is offered on a per-host basis. Several different capacity types are supported as shown in the table below. The capacity type determines which kind of VMs and how many VMs can be provisioned on those hosts, as indicated by the Consumption Units and Max VMs in the table below. Hosts are bundled together in clusters (known as "Horizon Pods") of up to 32 hosts of the SAME capacity type. A tenant will have one or more Horizon Pods. Each capacity type requires its own Horizon Pod. Each Horizon Pod can support up to 2,000 provisioned VMs. Horizon Cloud Service on IBM Cloud provides the following capacity types on these hosts:

Capacity Type	Standard Capacity	Hosted Application Capacity	M60 Professional	M60 Premium	M60 Performance
Host Type	Standard Host	Standard Host	vGPU Workstation (M60)	vGPU Workstation (M60)	vGPU Workstation (M60)
Usage Type	VDI	RDSH Apps and Published Desktops	VDI	VDI	VDI
Min Hosts Per Pod	2 (1 Usable)	2 (1 Usable)	1	1	1
Max Hosts Per Pod	32 (30 Usable)	32 (30 Usable)	32	32	32
High Availability / SLA in effect	Yes	Yes	No	No	No

Capacity Type	Standard Capacity	Hosted Application Capacity	M60 Professional	M60 Premium	M60 Performance
Max VMs Per Host[1]	18 to 210 (210 SDCs)	10 (10 RDCs)	16 (16 M60s)	8 (16 M60s)	4 (16 M60s)
# of VM Models Supported	4	1	1	1	
VM Model Consumption Units	SDC (1 vCPU, 2GB vRAM, 30GB HD)	RDC (8 vCPU, 32GB vRAM, 240GB HD)	M60 (4 vCPU, 16GB vRAM, 120GB HD, 2GB vGPU)	M60	M60

High Availability is only available with the Standard Host which is why a minimum pod size is two hosts, and in a maximum pod size of 32 hosts the actual usable capacity is 30 hosts. One High Availability host is required for every 15 (or up to 15) hosts in the pod. Because of the capacity reserved for High Availability, usable capacity will always be one fewer hosts than the pod possesses. Each Standard Host pod must have one or two High Availability hosts, depending on the size of the pod.

Example: Company ABC wants to deploy a tenant for 800 value desktops, 30 RDSH servers, and 50 M60 Professional Desktops (1 Value Desktop consumes 1 SDC unit). For this tenant, the customer will need to purchase the following capacity entitlement:

- Round Up (800/210) + 1 HA Host = 5 Standard Hosts
- Round Up (30/10) + 1 HA Host = 4 Standard Hosts
- Round Up (50/16) = 4 M60 Hosts
- Total: 9 Standard Hosts and 4 M60 Hosts.

Once provisioned as a capacity type, making changes to hosts and capacities within a tenant will require contacting VMware. Any hosts being modified for use for a different capacity type must be cleared of all VMs prior to re-assignment. Capacity type can only be changed within what the host supports; for example, a Standard Host will only allow customers to shift usage from Hosted Apps Capacity to Standard Capacity, and vice versa. Capacities and types cannot be adjusted across tenants.

Similarly, pods of the same host or capacity type in the same tenant can be adjusted with respect to the host count of each pod. For example, a tenant with both an M60 Professional Pod and a M60 Premium Pod could move hosts between those two pods as their use cases adjust. Those adjustments require contacting VMware.

All capacity types are deployed, by default, on dedicated computing servers with layer-2 network isolation for workload traffic isolation, dedicated storage volumes, and a dedicated desktop management instance. Each Horizon Cloud Service on IBM Cloud instance is deployed with a public IP address for VPN-less remote access directly from the internet. Desktops and published applications can be accessed through the Horizon Client, Horizon HTML Access, or Workspace ONE Access.

Horizon Cloud Service on IBM Cloud - Standard Capacity Model Options on Standard Host

The **Standard Desktop Capacity** (“SDC”) unit contains one vCPU, 2GB vRAM, 30GB Hard Disk capacity, and 20 storage IOPS. Customers can provision desktop VM instances based on predefined models that consume one or more SDC units. For example, a customer that purchases a 12-month subscription for one Standard Host can

[1] Maximum VMs per host is determined by desktop models selected and assumes a fully provisioned host with no platform, utility, imported, or image VMs present on the host. Actual usable capacity may vary due to specific tenant conditions. Note that Standard Capacity is the only capacity type with more than one model available for provisioning.

provision between one and 150 Value Desktop VMs, or between one and 75 Professional Desktop VMs, or 37 Premium Desktop VMs, or a mixture of VMs of different model types at any time during that 12-month term (actual host capacity may vary due to other workloads required by the customer such as images, imported VMs, and customer managed utility server VMs). Customers can provision VMs with any predefined desktop model so long as the customer has sufficient IBM Cloud host capacity to satisfy the provisioning task.

Standard capacity desktops are available in four predefined SDC models:

- **Value Desktop** provides one vCPU, 2GB vRAM, 30GB HD, 20 IOPS.
- **Professional Desktop** provides two vCPU, 4GB vRAM, 60GB HD, 40 IOPS, and the benefits of Soft3D for the end user.
- **Premium Desktop** provides four vCPU, 8GB vRAM, 120GB HD, 80 IOPS, and the benefits of Soft3D for the end user.
- **Performance Desktop** provides eight vCPU, 16GB vRAM, 240GB HD, 160 IOPS, and the benefits of Soft3D for the end user.

The default model specifications fit common workloads and ensure optimal usage of the assigned capacity. On request, there is the ability to assign non-standard desktop models under pre-determined conditions.

Horizon Cloud Service on IBM Cloud - Hosted Applications Capacity Service Model Options on Standard Host

Hosted Applications Capacity VMs are available in the following models:

- **Hosted Apps Server** provides eight vCPU, 32GB vRAM, 240GB HD, 160 IOPS, and the benefits of Terminal Services and Published Applications for the end user.

A Standard Host can run up to 7 Hosted Apps Server VMs. User density will vary by application payload and user requirements. When provisioning for Hosted Application Capacity, a customer must designate how much space to reserve for images.

The default Apps Server model specifications fit common workloads and ensure optimal usage of the assigned capacity. On request, there is the ability to assign non-standard desktop models under pre-determined conditions.

Horizon Cloud Service on IBM Cloud - Graphical Workstations Service Model Options

Horizon Cloud Service on IBM Cloud allows customers to purchase and provision vGPU-backed desktops and workstations.

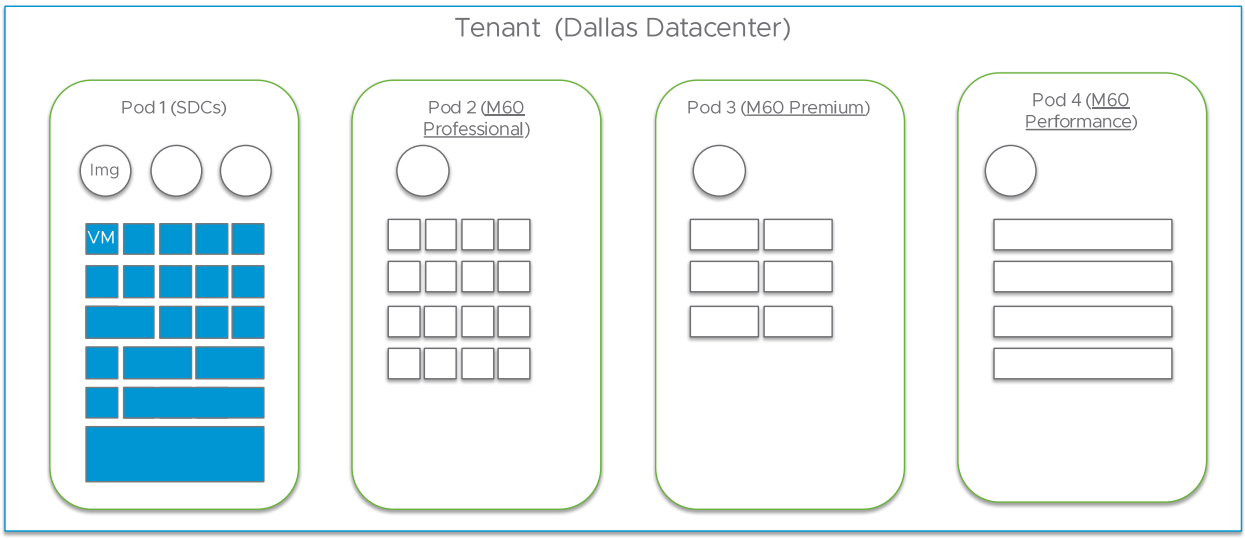
The following desktop models are available for provisioning within each vGPU capacity type:

M60 Workstation workloads are available in three predefined models:

- **Professional** provides four vCPU, 16GB vRAM, 120GB HD, 2GB vGPU Memory
- **Premium** provides eight vCPU, 32GB vRAM, 240GB HD, 4GB vGPU Memory
- **Performance** provides sixteen vCPU, 64GB vRAM, 480GB HD, 8GB vGPU Memory

vGPU desktops and workstations are provisioned in full hosts only; each model's host capacity is set forth in the table, above. A pod (a logical container of capacity, images, and subnets) can contain one or more hosts. vGPU model capacities are not interchangeable within a host and cannot be mixed within a pod. Because you cannot easily modify the capacity allocated to a particular model type after it has been provisioned, it is important to size pods with vGPU models by planning how many hosts each pod should contain, based on the desired desktop models for that host. For example: if you are planning to deploy some number of standard desktops (i.e., not vGPU desktops), 16 Professional M60 desktops, 6 Premium M60 desktops, and 4 Professional M60 Workstations, you would allocate your tenant capacity as four pods, each with sufficient hosts for model capacity desired.

As an example, see the following graphic:



If you need to re-allocate your pod capacity for a different model configuration, you may do so by contacting VMware support. For further questions regarding planning for vGPU Desktops and Workstations, consult your VMware End User Computing ("EUC") sales engineer.

All model specifications are fixed and cannot be adjusted.

IMPORTANT NOTES:

- vGPU desktops and workstations are exempt from the Service Level Agreement applicable to the service.
- Use of vGPU VMs requires NVIDIA licenses. Customers are responsible for providing their own NVIDIA software licenses. See the following links more information regarding NVIDIA licensing and installation requirements:
  - https://images.nvidia.com/content/grid/pdf/161207-GRID-Packaging-and-Licensing-Guide.pdf
  - https://docs.nvidia.com/grid/latest/grid-license-server-user-guide/index.html

Horizon Cloud Service on IBM Cloud - Starter Edition

Customers wanting to do a short-term proof of concept for the Horizon Cloud Service on IBM Cloud offering can purchase the Starter Edition subscription, which comes with 50 concurrent user entitlements, and either 120 Standard Desktop Capacity units or 5 Hosted Application Capacity units on a Standard Host as determined at tenant provisioning time. Customers can connect to their corporate networks using VPN. The Starter Edition also has a specialized onboarding package.

To maintain a low cost, simple, and quick deployment, the Starter Edition comes with some limitations. The Starter Edition does not have a High Availability SLA, cannot incorporate additional add-on features or functions, and cannot use direct connect functionality such as MPLS or Equinix Cloud Exchange. Customers deployed on the Starter Edition can convert to full production environments by purchasing a subscription to the regular service SKUs (both user and capacity) and will not need to reconfigure their tenant environment. An upgrade to a production tenant instance with High Availability will require a maintenance window and coordination with VMware.

Horizon Cloud Service on IBM Cloud - Image Templates

In order to provision workloads, customers must use image templates - whether provided by VMware or by the customer. Images must be configured and optimized according to VDI (virtual desktop infrastructure) best practices in order to properly function and perform in the Horizon Cloud Service on IBM Cloud environment. Image templates typically consume host storage when powered off, but will also consume CPU capacity and memory on

the host when powered on for editing and publication. During onboarding, customers will be required to set an image quota (number of images they will maintain) so that sufficient capacity on the host is reserved for provisioned workloads.

All utility servers must be sized to one of the predefined desktop model hardware specifications, and will consume workload units based on the size selected except as noted in Appendix B.

VMware will provide a catalog of supported virtual desktop Image Templates that you may deploy into your Horizon Cloud Service on IBM Cloud environment. The deployment and use of such templates will be subject to the Third Party Terms located at:

http://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/support/vmware-horizon-cloud-hosted-third-party-terms.pdf.

VMware will provide these templates, test them for quality, check for viruses, and install security patches before making them available in the Horizon Cloud administration console. VMware will also maintain and update these templates from time to time. You are responsible for deploying and configuring the virtual desktop Image Templates that you choose to use, activating related licenses, and maintaining compliance with the applicable license terms.

To comply with VMware's legal obligations to our third-party licensors, you will not be permitted to export, download, or remove certain templates or any installed forms of certain templates for installation or use outside of the Horizon Cloud Service on IBM Cloud service. For more details regarding the licensing of Desktop Image Templates, please see the Third Party Terms.

You may implement or import your own Image Templates so long as you have the legal right to deploy and use the software contained in those templates.

Templates that are provided by VMware but that are infrequently used, out-of-date, or no longer supported may be removed at any time.

Horizon Cloud Service on IBM Cloud - Template Upload

Horizon Cloud Service on IBM Cloud allows custom templates. All templates must use Open Virtual Machine Format (OVF). Customers can coordinate with VMware to upload any custom templates. Once transfer is completed, VMware will mount the received template into the customer account, and thereafter it will be usable as an Image Template.

Horizon Cloud Service on IBM Cloud - Add-On Storage

Add-on storage is required to use advanced functions such as the VMware Dynamic Environment Manager™ (to store user settings and user profiles). Add-on storage can be allocated to utility server VMs as one additional disk mount. Utility server E:/Drive maximum size is limited to 12000GB of raw storage; actual usable storage may vary due to many factors. If an individual hard disk is greater than 1000GB, storage can be purchased in increments that are greater than the largest hard disk. Those increments are 1000, 2000, 4000, 8000, and 12000GB.

Customers may choose to buy additional hard disk storage entitlements, in 1000GB increments (referred to as 1TB in the actual SKUs); however, existing hard disks (such as utility server drives) cannot be expanded.

Horizon Cloud Service on IBM Cloud - VMware Dynamic Environment Manager

For the Horizon Cloud Service on IBM Cloud offering, VMware Dynamic Environment Manager must be installed as a separate utility server VM inside the Horizon Cloud Service on IBM Cloud tenant, and will require a network file share to be established to save system and user settings.

The VMware Dynamic Environment Manager feature requires a utility server and purchase of additional storage capacity in the amount of the customer's expected usage (typically between 125MB to 150MB per user).

Add-on storage can be purchased in 1 Terabyte increments and allocated in 1, 2, 4, 8, and 12 TB LUNs. Add-on storage performs at 1.5 IOPS per gigabyte.

Please consult with your VMWare EUC sales engineer regarding planning for use of VMware Dynamic Environment Manager with the Horizon Cloud Service on IBM Cloud.

Horizon Cloud Service on IBM Cloud - Utility Servers

Horizon Cloud Service on IBM Cloud utility VMs are intended for use with desktop and Terminal Services applications in direct support of the VDI and remote application service delivery functions. An exception is made for customers that wish to use a VM instance as a utility server (such as domain controller, active directory server, DHCP relay or file server). Anti-virus and OS lifecycle management tools (such as SCCM) are also allowed in limited quantities, but are not recommended due to their transactional nature and potential adverse impact on performance of desktop VMs. To protect the integrity of the Horizon Cloud Service on IBM Cloud offering, VMware reserves the right to limit the resources available to the utility server, or to require the customer to upgrade the utility server specification (by consuming additional SDC units), or ultimately to remove the utility server from the tenant environment. Utility servers have the following administration limitations:

- They will be initially deployed by VMware by using an existing catalog image or customer-provided image.
- All utility servers must fit within the specification of an existing desktop model specification.
- All utility servers must be compatible with the underlying VMware vSphere® host version on which they will be deployed. Maintaining OS compatibility through vSphere host upgrades is a customer responsibility.
- Utility servers can only be deployed with a single Network Interface Card (NIC).
- Max E:/Drive size per utility server is 12TB.
- E:/Drives can only be allocated in 1, 2, 4, 8, and 12TB sizes.
- The utility servers can only be accessed either internally from the customer environment or via the console.
- The utility servers can only be administered by an authorized customer administrator accessing the VM directly via remoting protocol or via built-in web application running on the server
- There is no ability to customize the utility servers' deployment configuration with regards to networking, availability, load management, infrastructure performance or business continuity
- Number of utility servers allowed:
  - Up to 200 SDC units: 3
  - Up to 1,000 SDC units: 6
  - Plus one additional utility server for every additional 1,000 SDC units purchased.
  - These numbers do not include utility servers specifically used with VMware Dynamic Environment Manager.
- The following are not supported for utility servers:
  - Load balancing, NATs, or custom firewall rules: Utility servers are intended to run applications that support cloud desktop deployments. They are not designed to support server applications that require public internet access or advanced infrastructure configurations.

One VM in the tenant environment may be used as a utility server (with a Professional Desktop VM specification) without drawing from the SDC quota purchased. Any increases to the free utility server or additional utility servers will count towards the desktop quota purchased by subtracting the total CPU and memory resources consumed for utility servers as expressed in terms of whole number of desktops from the total VMs purchased.

Except for approved utility server functions, any use of server-based applications or transactional applications is not supported, and may interfere with performance and user experience. Utility servers may not intercept network communications between the provisioned VMs and platform components. Encrypted hard disks are not allowed within the customer's VM environment. Customers that need secure disk services should consider redirecting user data to their data center or should purchase a separate IaaS cloud instance and deploy an encrypted file server for user data.

Utility server recommendations for entry level enterprise accounts (up to four standard hosts: 400 SDCs and 200 users):

Recommendation	Server Function	vCPU	GB RAM	GB HD
Basic	AD/DNS/DHCP #1	2	4	60
Basic	DEM/AAU/Fileshare #1	2	4	60 (to 0.5TB with add-on storage)
Basic	WS1 Connector #1	4	8	50
HA	AD/DNS/DHCP #2	2	4	60
HA	DEM/AAU/Fileshare #2	2	4	60 (to 0.5TB with add-on storage)
HA	WS1 Connector #2	4	8	50

DEM = Dynamic Environment Manager
AAU = Agent Auto Update

Horizon Cloud Service on IBM Cloud - Virtual Machine Types

Horizon Cloud Service on IBM Cloud supports the creation of VMs through use of Full Clone-based and Instant Clone-based provisioning. There are advantages and disadvantages to each type. A customer must make that choice when base images are created. Images can only be created for use as one type (not both). The type of VMs provisioned in a pool will depend on the image selected.

Instant Clone VMs provision very quickly (in minutes) but have the following image limitations:

- An Instant Clone image can only provision desktop instances to a single domain chosen at image publish time. If you have more than one domain, you will need an equivalent number of images even if they are identical in content.
- Only Windows 7 and Windows 10 client operating systems are supported.
- Maximum of two monitors with maximum display resolution of 2560 x 1600 pixels.
- Best used for Non-Persistent / Floating desktop use cases.
- If a customer intends to provide a “dedicated” desktop experience, an Instant Clone desktop is best used together with VMware Dynamic Environment Manager.

Full Clone VMs provision at a much slower rate and are familiar to individuals with VDI background as the classic dedicated / persistent desktop experience. Full Clone VMs can also be used for Windows Server VDI desktops as well as Remote Desktop Session Host (“RDSH”) Hosted Application Servers.

Horizon Cloud Service on IBM Cloud -- Usage Restrictions

Load Testing

Customer load testing (such as automated or manual login stress tests) is prohibited without prior approval from and coordination with VMware. Customers that wish to perform such tests must submit a support ticket and coordinate the planning of those tests with VMware to ensure minimal interference with performance and user experience.

SMTP Port 25

VMware will not allow port 25 egress out of the VMware-provided internet connection. TCP Port 25 (usually used for SMTP) is subject to egress filtering and not allowed for usage, with no exceptions. A customer can use port 25 on VPN or Direct Connect.

Network Management

Customers will not have access to a Horizon Cloud Service on IBM Cloud edge (router) appliance, and will not have any ability to configure or customize the firewall and network address translation rules set and managed by VMware.

Dedicated connectivity active/passive redundancy (via BGP only) is supported, but the customer will have to choose which link is active and which link is the backup, and also will be responsible for configuration to accomplish auto-failover of link in case of active link down.

Customers may request up to 10 desktop networks to be available in the tenant environment, and up to 10 VPN connections to that tenant.

In-guest VPN usage is not allowed, and will block VMs from being accessible by end users.

4.2 Horizon Cloud Service on IBM Cloud Capabilities

The Horizon Cloud Service on IBM Cloud offering includes the following capabilities:

- **Domain Binding** via the Horizon Cloud administration console to set up active directory, administrator roles and permissions, and end user groups.
- **Image Templates** may also be managed through the Horizon Cloud administration console and are used as the base image from which VMs are cloned.
- **Desktop Pools** are the grouping object for VMs, RDSH-published desktops, and RDSH-published applications. Pools specify which model, image, VM type, and other policies to apply when creating VMs. Desktop VMs can only be created as part of a pool.
- **RDSH Published Desktops (Sessions)** are the published desktops running on hosted RDSH servers that are accessed by the end user.
- **RDSH Published Applications (Apps)** are the published applications running on hosted RDSH servers that are accessed by the end user.
- **Horizon Pod** for Horizon Cloud Service on IBM Cloud is a logical container which has capacity, images, and subnets available to that pod. Pools provisioned in the pod are limited in size by the pod's capacity and limited in content to the images available in that pod. VMs are attached to subnets associated with a pod. By default, capacity, images and subnets are unique to a pod. Customers can request for pods to have image syncing, which can (depending on the specific use case) eliminate the need to copy images across pods. The type of capacity attached to a pod determines which desktop model types can be provisioned in that pod.
- **Cloud Monitoring** is used to capture and display guest VM performance and usage statistics

4.3 Horizon Cloud Service on IBM Cloud - Service Portals

Horizon Cloud Service on IBM Cloud includes access to three self-service consoles:

- **My VMware Account Management Console** provides access to subscription status, integrating navigation, viewing and management of all VMware product entitlements and support under a single account. It also allows for download of the Horizon Service software components.
- **VMware Horizon Cloud Administration Console** is the primary interface for consumption and management for the Horizon Cloud Service on IBM Cloud offering, including domain binding, image management, desktop provisioning, end user entitlement, and multi-factor authentication under the same sign-on.
- **VMware Horizon® HTML Access™ Portal** is the primary web interface for end users accessing the desktop and published apps. This interface provides browser-based access via HTML5. Users are not required to use the portal to access their desktop or app – they can do so with the Horizon Client that is

supported on Windows, Mac, Linux, iOS, Android, and through various third-party thin clients and zero clients.

VMware will also provide organization administrator access to the Horizon Cloud Service on IBM Cloud application programming interface (API) for programmatic resource management. Documentation is provided upon request.

4.4 Horizon Cloud Service on IBM Cloud - Service Operations

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

4.4.1 IBM Account

You will not be able to access or use the Service Offering without having your own customer account with IBM (an "IBM account"), which you must establish directly with IBM. This means that if you do not already have an IBM account, you must establish one prior to being able to access and use the Service Offering. See https://www.ibm.com/support/customer/csol/contractexplorer/cloud/csa/us-en/10 for the current form of the IBM Cloud Services Agreement. If you have questions on the IBM agreement, you must contact IBM.

4.4.2 Horizon Cloud Service on IBM Cloud - Support

VMware will provide support for problems that you report and selected additional services to assist with adoption of and related to the service. VMware will only provide support for Horizon Cloud Service on IBM Cloud workloads. Support may be provided in any country in which VMware or its providers maintain facilities. If you provide Content (as defined in the Terms of Service) in connection with support requests, VMware will handle that Content in accordance with the Terms of Service. Support for customer-controlled infrastructure components such as a File Server, Directory Service, DNS, and NTP, is not included.

For Horizon Cloud Service on IBM Cloud, supported versions include the latest three production release versions. Customers on older tenant versions will not be eligible for support and are encouraged to keep up with the VMware change management requests.

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

4.4.3 Horizon Cloud Service on IBM Cloud - Provisioning

VMware will provide the following provisioning services for the Horizon Cloud Service on IBM Cloud offering:

- Implementation of service components (physical servers, physical storage, and physical network devices) needed to support contracted resource pools.
- Providing initial network resources including default public IP addresses.
- Providing initial capacity resources for Desktop Models (memory, processing, primary storage, and networking) and Hosted Apps Servers.
- Enabling a secure point to point network interconnect (aka backhaul) via VPN or other dedicated connection from the Horizon Cloud Service on IBM Cloud network to your corporate network. Note that dedicated connectivity from your data center to VMware's port of access in VMware's data center is purchased separately from your carrier or telecommunications provider. Direct Connect from VMware's port of access to your tenant network (i.e., within the service) must be purchased separately (from VMware) and will have an additional monthly charge.

- Switching network interconnect from VPN to dedicated connection. Note that this conversion requires up to 14 days lead time after all connectivity elements are in place and the configuration has been validated by both VMware and the customer.
- Providing up to 10 VMware-approved 60GB (Professional Desktop) Images from the current Image catalog.
- Installing qualified utility server VMs in your Horizon Cloud Service on IBM Cloud environment (see "Usage Restrictions" in section 4.1).
- Providing utility server for network share use with VMware Dynamic Environment Manager (Note: purchase of add-on storage required).
- Providing access to self-service training videos.
- Providing up to two hours of Horizon Cloud administration console and VMware Horizon HTML Access Portal walkthrough.
- Validating tenant setup by provisioning a desktop with a VMware-provided image template.

You will be responsible for the following provisioning services:

- Providing corporate resource assistance for establishing site-to-site network connectivity.
- Customizing Image Templates.
- Creating desktop, session, native and RDSH application pools and assigning to users.
- Installing and configuring custom or third-party applications and operating systems on Image Templates or deployed VMs.
- Configuring and supporting utility server VMs.
- Configuring and supporting an NTP server usable by the Horizon Cloud tenant if using quad zero network routing (0.0.0.0) where all network traffic is routed via your corporate network.

4.4.4 Horizon Cloud Service on IBM Cloud - Disaster Avoidance and Disaster Recovery

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

- Data protection, such as routine backups for the Horizon Cloud infrastructure, including management and user-management interfaces owned and operated by VMware.
- Data and infrastructure restoration for the Horizon Cloud infrastructure, including management and user-management interfaces owned and operated by VMware.
- NOTE: VMware does not provide backup or recovery for any customer-managed assets such as customer-provisioned VMs and Images.

You are responsible for the following services with respect to disaster avoidance and disaster recovery:

- Data protection, such as routine backups, for the data and content accessed or stored on Horizon Cloud Service on IBM Cloud VMs or storage devices, configuration settings, etc.
- Data, content, VM, and configuration restorations for assets accessed or stored on your Horizon Cloud Service on IBM Cloud account.

4.4.5 Horizon Cloud Service on IBM Cloud - Monitoring

VMware will provide the following services with respect to monitoring:

- Monitoring the infrastructure, infrastructure networks, top-layer management and user-management

interfaces, and compute, storage and network hardware for availability, capacity, and performance. VMware will also provide customers with a service summary level view of desktop model quota utilization and desktop state.
- Horizon Cloud Service on IBM Cloud data center status can be viewed at: http://status.horizon.vmware.com/

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

- Monitoring the assets deployed or managed within your Horizon Cloud Service on IBM Cloud tenant infrastructure, including, but not limited to inside the guest operating systems, applications, inside the guest storage utilization, dedicated network connectivity / VPN, or application vulnerabilities, etc.
- Monitoring the assets deployed within your own corporate infrastructure that are critical to Horizon Cloud on IBM Cloud tenant operations, including, but not limited to Domain Controller, Active Directory, DHCP, VPN, and user roles and permissions.

4.4.6 HORIZON CLOUD SERVICE ON IBM CLOUD - INCIDENT AND PROBLEM MANAGEMENT

VMware will provide incident and problem management services (e.g., detection, 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 servers, storage and network devices.
- Service software over which VMware has provided the customer administrative access and control, such as the VMware Horizon Cloud Administration Console.
- VMware-provided operating system templates to the extent that:
  - Published templates cannot be accessed
  - Published templates cannot be used for provisioning without modification
  - Published templates cause errors at first run time
  - There are substantial hangs or excessive delays in the retrieval of a template
  - The configuration of a published template affects the virtual machine's interaction with the hypervisor
  - Time synchronization issues (NTP) exist

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, 2-factor authentication).
- User-deployed and configured assets such as VMs, VMware Dynamic Environment Manager, 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 even if the source is supplied from VMware. For any operating system issues, please contact your operating system support organization.
- VPN integration.
- Performance of user-deployed VMs, VMware Dynamic Environment Manager, custom or third-party applications, your databases, operating systems imported or customized by you, or other assets deployed and administered by you that are unrelated to the Horizon Cloud Service on IBM Cloud offering.
- Anything else not under the direct control and administration of VMware.

4.4.7 HORIZON CLOUD SERVICE ON IBM CLOUD - CHANGE MANAGEMENT

VMware will provide the following change management elements:

- Processes and procedures to maintain the health and availability of the Horizon Cloud administration console and the service components.
- Processes and procedures to release new code versions, hot fixes, and service packs related to the Horizon Cloud administration console, and Horizon Cloud service components.
- Notifications of service upgrades required by a certain date and time and requests for scheduling of maintenance windows before that time. VMware will attempt three scheduling requests to coordinate an appropriate time for the maintenance. If no response is provided within 48 hours of the third attempt, VMware will automatically schedule that upgrade if you fail to respond to the scheduling request, or if you and VMware cannot agree on an earlier date and time before specified date and time.

You are responsible for:

- Management of changes to your VMs, VMware Dynamic Environment Manager, operating systems, custom or third-party applications, and administration of general network changes within your control.
- Administration of self-service features provided through the Horizon Cloud administration console, up to the highest permission levels granted to you, including but not limited to VM and domain functions, backup administration, and general account management, etc.
- Cooperating with VMware when scheduled or emergency maintenance is required.
- "Scheduled maintenance" is defined as pre-scheduled maintenance that has the potential to impact the availability of the customer's environment.
  - Maintenance Windows: Scheduled maintenance is generally performed between the hours of 12:00AM (Midnight) to 6:00AM local data center time. However, on rare occasions it may be necessary for VMware to perform maintenance outside of this window, and VMware reserves the right to do so.
  - Advance notice: A minimum of 24 hours advance notice will be given for scheduled maintenance.
- "Emergency maintenance" is defined as potentially impactful maintenance activity that must be executed quickly due to an immediate, material threat to the security, performance, or availability of the Horizon Cloud Service on IBM Cloud offering. Every attempt will be made to provide as much advance notice as possible, but notice depends on the severity and critical nature of the emergency maintenance.

4.4.8 HORIZON CLOUD SERVICE ON IBM CLOUD - SECURITY

End-to-end security of the Horizon Cloud Service on IBM Cloud offering is shared between VMware and you. VMware will provide security for the aspects of the service over which we have sole physical, logical, and administrative level control. You are responsible for the aspects of the service 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 service from physical security breaches.
- **Information Security:** Protection of the information systems used to deliver the service 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 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.

- **Patching and Vulnerability Management:** VMware will maintain the systems it uses to deliver the service, 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. 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. 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.
- **Security Monitoring:** You are responsible for the detection, classification, and remediation of all security events that are isolated within your service environment, 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.
- **Compromised Desktops**: Any compromised desktops and resolving related issues. VMware reserves the right to suspend desktops or whole customer accounts if compromised desktops are detected, to protect VMware's infrastructure and business operations.

4.4.9 Horizon Cloud Service on IBM Cloud - Data Access

In the event of issues that require diagnosis and troubleshooting, select personnel from the VMware Horizon Cloud Service operations team will have the ability to remotely log in to the Horizon Pod 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 Pod, which will show usernames, 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 within the Horizon Cloud Service on IBM Cloud offering.
  - Have real-time access to the current operational health status of the Horizon Cloud Service on IBM Cloud offering.
- 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 to disable this if desired.
- VMware will be storing information that includes customer contact information (name, email), Horizon Pod data such as location, and audit information that covers life cycle events.
- Transmission of the files from the Horizon Pod to the Horizon Cloud Service on IBM Cloud service infrastructure is done over an SSL channel, but the files themselves are not encrypted at rest.

4.5 Capacity and Services for Horizon Cloud Service on IBM Cloud

Capacity orders for Horizon Cloud Service on IBM Cloud include Host Capacity, IP Address, and Internet Bandwidth components for a single service instance ("Service Identifier" or "SID") as described in further detailed in Appendix B.

When you order capacity, you will be required to fill out a detailed provisioning questionnaire provided to you by VMware (via email or link to the online account configuration portal). The information you provide is required to provision your order. It is your responsibility to complete and return the questionnaire within 10 business days of submitting your order. Your subscription term and Billing Period will begin on the earlier of (i) the date the service has been provisioned or (ii) 60 calendar days after the order date (irrespective of whether you complete the provisioning questionnaire). If you do not provide a completed questionnaire, we will provision the order on a commercially reasonable basis. In that case, your subscription term will terminate one year after the beginning of the subscription term without further extension. VMware can elect to delay the start of the Billing Period at our discretion, and we will notify you via email if such action is taken.

Additional capacity or services, such as additional hard disk storage, may be purchased at the time of your initial order or through the My VMware portal at any time during the subscription term. Additional terms and fees may apply to such additional services. Those additional orders will terminate concurrently with the term of the initial order.

Account changes to capacity can be made by ordering additional capacity or services during the contracted subscription term. Consult your VMware sales representative for details and conditions on timing, pricing, and related matters.

Service capacity reductions must be coordinated with VMware at the time of subscription renewal and will require a new order for the reduced service capacity. However, if the capacity associated with your reduced service order is less than the capacity required to sustain your then-current workloads, VMware will continue to bill you for the excess capacity at then-current published rates until you have released the excess capacity and VMware has reclaimed it. Reduction orders must be submitted to VMware a minimum of 30 calendar days prior to the date of subscription renewal. Reduction orders on subscription terms less than 12 months must be submitted to VMware at least five calendar days prior to the date of subscription renewal.

Order contents are not considered available for use until fulfillment is fully acknowledged by VMware.

4.6 Add-On Capacity for Horizon Cloud Service on IBM Cloud

Add-on capacity (such as additional hosts and storage) may be purchased during the contracted subscription term to meet new or expanded requirements. Consult your VMware sales representative for details and conditions on timing, pricing, and related matters.

Additional desktop capacity and storage may be added via the My VMware portal or by issuing a purchase order to VMware or to your authorized VMware reseller.

The subscription term for add-on capacity or services will be set to terminate at the same time as the core subscription term for the SID.

5. Horizon Service - Business Operations

This section summarizes processes for ordering, scaling, renewing, suspending, and terminating any of the services.

5.1 Ordering and Invoicing

The Service Offering is sold on a per-user basis. Subscriptions are in quantities of 50 seats for initial purchases, and quantities of 10 seats for incremental (add-on) purchases This entitlement is purchased as a 1-, 12-, 24-, 36-, 48-, or 60-month subscription, for the specified number of seats. When a customer purchases an entitlement to the Service Offering, the customer can deploy the Service Offering as any one, or all, or any combination of, the three Horizon services described above). A customer can prepay for the entire committed subscription term, or can choose to be billed and pay monthly or annually. You may use the Service Offering for up to the number of users for which you have paid the applicable fees.

NOTE: As referenced in the VMware Product Guide, please note that, if you receive your entitlement to Service Offering through the Horizon Universal License SKU, under the Subscription Upgrade Program for Horizon, you

agree to relinquish your entitlements to corresponding Horizon perpetual licenses. You must not use any license keys related to those perpetual licenses, and VMware will invalidate those keys. You are not required to uninstall any Software if you convert your existing Horizon perpetual licenses deployment to Horizon Service entitlements by installing the Horizon 7 Cloud Connector and managing licenses through the Horizon Cloud control plane.

Subscription Ordering and Deployment

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 (unless otherwise provided in the applicable order document). This billing relationship may be modified at renewal.

An active subscription to the Service Offering entitles customers to deploy the purchased seats on any of the three individual services: that is, Horizon Cloud Service on IBM Cloud, or Horizon Cloud Service on Microsoft Azure, or Horizon 7 subscription. For example, if a customer purchases an entitlement to 1,500 seats, the customer is entitled to use 500 seats for each service, or to use these seats across any combination of deployments, but not exceeding a total of 1,500 seats.

Additional seats may be purchased at the time of your initial order or at any time during the Subscription Term. Consult your VMware sales representative for details and conditions on timing, pricing, and related matters.

For Horizon Cloud Service on IBM Cloud, customers will be required to purchase IBM Cloud capacity from VMware. Customers may purchase additional IBM Cloud capacity; consult your VMware sales representative for details and conditions on timing, pricing, and related matters.

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 provided.

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

Provisioning

For Horizon 7 subscription and Horizon Cloud Service on Microsoft Azure, it will take no longer than 5 days to provision your order. The Subscription Term and the applicable billing period will begin within 24 hours of the date the Service Offering has been provisioned.

For Horizon Cloud Service on IBM Cloud, the current service level commitment is to provision the service within 14 days from receipt of the order barring any delays from the customer or customer’s environment. For orders that include capacity for IBM Cloud, the Subscription Term and the applicable Billing Period will begin within 24 hours of the date the Service Offering has been onboarded, or 60 days after the date of the order, whichever first occurs. VMware can elect to delay the start of the Billing Period at its discretion.

5.2 RENEWAL

VMware reserves the right to not renew any SID at the end of its subscription term, in which case we will notify you 30 days prior to the end of the subscription term. Renewal options for each SID may be selected using the My VMware administrative portal.

Auto-Renewal (the default setting)

Except as set forth in this Section 5.2, each SID will automatically renew. You may opt out of auto-renewal by changing your renewal option setting for the SID within the My VMware Portal available at https://my.vmware.com. The deadline to change the renewal option is 30 days prior to the last day of the then-current SID subscription term.

Modify Subscription on Renewal

If you select the renewal method “Modify”, you will be contacted prior to the end of the Subscription Term to discuss your renewal options. Selecting “Modify” as the renewal method setting allows you to modify your Service Offering configuration and to make changes to your reseller relationship, if applicable, by both changing your setting for the SID within the My VMware Portal available at https://my.vmware.com and by issuing a new purchase order. If you do not make any changes to your current SID profile and/or you do not issue a new purchase order for the new Service Offering to VMware or to your VMware authorized reseller (if applicable) by the deadline specified below, then your existing SID, as then 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 elect a change in your reseller relationship for that specific SID. The deadline to change the renewal option is 30 days prior to the last day of the current SID subscription term.

Terminate at End of Subscription Term

You may terminate your existing SID subscription by changing your setting for the SID within the My VMware Portal (available at https://my.vmware.com) to “Cancel”. When this option is set, your access to the Service Offering will expire at the end of the SID subscription term. The deadline to select the termination option is 30 days prior to the last day of the current SID subscription term.

5.3 Suspension and Re-Enablement

While a SID is suspended by VMware as described 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.

5.4 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, support and a deletion of such environments, configurations and data pursuant to applicable VMware policies.

Customer account contact data from a terminated SID will be deleted upon request.

APPENDIX A – HORIZON SERVICE OVERVIEW

Horizon Service	
VMware Horizon® 7 subscription	VDI and RDS desktop and application delivery on the customer's own infrastructure, either on-premises or VMware Cloud on AWS
VMware Horizon® Cloud Service™ on Microsoft Azure	Windows 10 VDI and RDS desktop and application delivery on the customer's own Microsoft Azure infrastructure capacity
VMware Horizon® Cloud Service™ on IBM Cloud	VDI and RDS desktop and application delivery on IBM Cloud, managed by VMware
VMware Horizon® Cloud Manager™	VMware hosted console to orchestrate and manage the customer's virtual workloads.
VMware Horizon® Client™	Allows end users to connect to and use virtual desktop and RDS desktops and applications from client end points
VMware Horizon® HTML Access™	Allows end users to connect to and use virtual desktops and RDS desktops and applications from a supported Web browser
VMware vSphere® Desktop	On-premises server virtualization for VMware Horizon® 7 on-premises capacity
VMware vCenter Server® for Desktop	On-premises manager for vSphere Desktop
VMware vSAN for Desktop Advanced	On-premises scalable storage for virtual desktops and RDS desktops and applications for VMware Horizon® 7 on-premises capacity.
VMware Horizon® 7 Cloud Connector™	Virtual appliance required for Horizon 7 Subscription that pairs the environment to the Horizon Cloud control plane
VMware 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 can be installed on the virtual desktops and RDS servers
App Volumes Agent**	
Horizon Agent	
VMware Dynamic Environment Manager™ Agent	
VMware Dynamic Environment Manager™	Stand-alone console for Dynamic Environment Manager
VMware Workspace ONE® Access™	Optional service that allows for single sign-on (SSO) for Horizon apps and desktops, ensures security with multi-factor authentication and control conditional access

**DaaS Agent is applicable only for Horizon Cloud on Microsoft Azure and Horizon Cloud on IBM Cloud*

***App Volumes Agent is applicable only for Horizon 7 Subscription*

Horizon Service Apps Subscription – RDS

	Horizon 7 Subscription	Horizon Cloud Service on Microsoft Azure	Horizon Cloud Service on IBM Cloud
Windows Virtual Desktops	No	No	No
Linux Virtual Desktops	No	No	No
Published Apps and Session-based Desktops	Yes	Yes	Yes
Virtualization Pack for Skype for Business	Yes	Yes	Yes
Instant Clone Technology	Yes	No	No
Session Collaboration	No	No	No
Help Desk	Yes	Yes	Yes
Dynamic Environment Manager	Yes	Yes	Yes
App Volumes	Yes	No	No
VMware vSAN for Desktop Advanced	Yes	No	No

Horizon Service Subscription – VDI+RDS

	Horizon 7 Subscription	Horizon Cloud Service on Microsoft Azure	Horizon Cloud Service on IBM Cloud
Windows Virtual Desktops	Yes	Yes	Yes
Linux Virtual Desktops	Yes	No	No
Published Apps and Session-based Desktops	Yes	Yes	Yes
Virtualization Pack for Skype for Business	Yes	Yes	yes
Instant Clone Technology	Yes	No	Yes
Session Collaboration	Yes	No	No
Help Desk	Yes	Yes	Yes
Dynamic Environment Manager	Yes	Yes	Yes
App Volumes	Yes	No	No
VMware vSAN for Desktop Advanced	Yes	No	No

APPENDIX B – HORIZON CLOUD SERVICE ON IBM CLOUD CAPACITY ORDERING

Ordering IBM Cloud Capacity

Host capacity SKUs can be purchased as Standard, M60, Storage, and network options (e.g., Direct Connect). Add-on SKUs purchased together with the core SKU will have the same subscription term as the related core licensing SKU; if purchased after the core SKU order, those add-ons will expire concurrently with the core SKU.

As an example, a new customer order could be as follows:

- Qty 1 Core Horizon Universal License Concurrent User Entitlement (50 users)
- Qty 5 Add-on Horizon Universal License Concurrent User Entitlement (10 users) (that is, an additional 50 users)
- Qty 4 Add-on Standard Capacity Host
- Qty 3 Add-on 1TB Add-on Storage

For example, a customer that has three tenants of standard capacity (West Coast Production, East Coast Production, and East Coast Staging) will require at least one core licensing SKU and 6 standard host SKUs, two hosts (or roughly 150 usable SDCs after HA) for each tenant. (Note that SKUs are defined at the region level, not at the data center level. A region may contain one or more data center locations.)

When purchased with Standard or Graphical Workstation Capacity, each tenant comes with the following standard options:

- IP Addresses: one public IP Address for access to the Administration Console and Desktop Portal/Broker
- Bandwidth: Each account is provided an aggregate bandwidth amount equal to the sum of desktop peak bandwidths as totaled from the standard desktop capacity quantities ordered. Average expected bandwidth is also listed for each model for customer remote site bandwidth planning purposes.

Standard Capacity Desktop Models

In order to provision desktop, the customer must decide which Desktop Model to use, which governs how much CPU, Memory, and Hard disk is allocated to such VMs, as well as potentially advanced option availability such as Soft3D. Each VM instantiated consumes one or more Standard Desktop Capacity (SDC) units as specified below.

Desktop Model	Value	Professional	Premium	Performance
vCPU	1	2	4	8
vRAM (GB)	2	4	8	16
vHDD (GB)	30	60	120	240
Average IOPs	20	40	80	160
Average Bandwidth (Kbps)	100	500	500	500
Peak Bandwidth (Kbps) per Core Size e.g. 50	1000	2,000	2,000	2,000
Soft3D Available	No	Yes	Yes	Yes
Workload Type	VDI	VDI	VDI	VDI

Desktop Model	Value	Professional	Premium	Performance
Windows 7,8 Client OS	Yes	Yes	Yes	Yes
Windows 10 Client OS	Yes	Yes	Yes	Yes
Windows Server OS	Yes	Yes	Yes	Yes
Standard Desktop Capacity	1	2	4	6

Example: An account with 150 standard desktop capacity will have 150Mbps of total aggregate bandwidth available for all the account's desktops

NOTE: Value desktops are not recommended to run Microsoft Windows 10 due to the amount of base memory consumed by the OS leaving very little additional memory available for applications without a severe performance degradation.

Due to service improvements and performance tuning, VMware reserves the right to modify the Hosted Apps Server specifications and quantities so long as the total capacity of Hosted Apps Servers purchased is of equal to or greater than the specification in this Service Description. Customers who provisioned an older specification of the RDSH server will be required to rebuild their pools to take advantage of the new specification, as mixed RDSH server specifications are not supported in a single tenant. Customers can still purchase the new specification SKUs and provision the old specification so long as equivalent resources (compute, memory, storage) were purchased for provisioning under the retired specification.

NOTE: Soft3D may only be used with compatible guest OS versions. vCPU performance is not restricted within each VM. vCPU is instead used as a factor in determining host density based on average consumption of 350Mhz per vCPU. Individual VMs are allowed to burst above 350 MHz per vCPU in order to ensure optimal aggregate performance. This could lead to potential resource contention and end user experience degradation on affected VMs. It is the customer's responsibility to ensure their VMs are properly sized to the appropriate desktop model to ensure sufficient resources are available to all VMs.

Hosted Application Capacity Models

The following is the specification for the Hosted Application Server:

Desktop Model	Hosted Application Server
vCPU	8
vRAM (GB)	32
vHDD (GB)	240
Average IOPs	320
Average Bandwidth (Kbps) per session	500
Peak Bandwidth (Kbps) per session	2,000
Soft3D Available	No

Desktop Model	Hosted Application Server
Workload Type	Published Desktops and/or Apps
Windows 7,8 Client OS	No
Windows 10 Client OS	No
Windows Server OS	Yes
Standard Desktop Capacity	8

Graphical Workstation Capacity Desktop Models

In order to provision graphical workstation VMs, the customer must decide which model to use; that governs how much CPU, Memory, and Hard Disk capacity is allocated to those VMs. Each VM instantiated consumes one or more M60 Workstation Capacity units as specified below.

Desktop Model	M60 Professional	M60 Premium	M60 Performance
vCPU	4	8	16
vRAM (GB)	16	32	64
vHDD (GB)	120	240	480
vGPU (GB)	2	4	8
Average IOPs	80	160	320
Average Bandwidth (Kbps)	500	500	500
Peak Bandwidth (Kbps) per Core Size e.g. 50	2,000	2,000	2,000
Workload Type	VDI	VDI	VDI
Windows Client OS	Yes	Yes	Yes
Windows Server OS	Yes	Yes	Yes
M60 Capacity	1	2	4

Due to how vGPU is associated with VMs, customers must specify (at the time of tenant deployment) the workstation models they plan to use on which hosts. Once operational, changes to this configuration can be requested by submitting a support request to VMware and are addressed on a best effort basis.

See Appendix C for Guest VM compatibility details.

Summary of Items Available for Purchase Separately

Available for purchase separately through *VMware Professional Services;* not included in the Service Offering:

- Onboarding Packages
- Project Management
- Use Case Assessment & Definition
- Desktop Engineering and Image Management
- Miscellaneous professional services requests

Additional services available for purchase from *third parties* that may be required to complete the setup of the Service Offering:

- Dedicated connectivity service from customer's data center to VMware's data center (up to four connections supported per location)
- Direct Connect setup inside the Service Offering data center to the customer's tenant instance

APPENDIX C - HORIZON CLOUD ON MICROSOFT AZURE GUEST OS COMPATIBILITY TABLE

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

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
Windows Server 2019		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 D – HORIZON CLOUD SERVICE ON IBM CLOUD GUEST OS COMPATIBILITY TABLE

Horizon Cloud Service on IBM Cloud supports the use of the following Windows operating systems on virtual machines hosted within the Service Offering.

Operating System	Patch / SP	32 / 64 bit	Additional Variants / Specs	VDI / RDSH	Instant Clone Capable
Windows 7	Base / SP1	Both	Professional / Enterprise	VDI	Yes
Windows 8.1		64	Professional / Enterprise	VDI	
Windows 10	See knowledge base link below for latest version support	64	Professional / Enterprise	VDI	Yes
Windows Server 2008 R2	SP1	64	Datacenter Edition	Both	
Windows Server 2012 R2		64	Standard, Data Center	Both	
Windows Server 2016		64	Standard, Datacenter	Both	

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/2149393

APPENDIX E – HORIZON 7 SUBSCRIPTION GUEST OS COMPATIBILITY

For Non-Windows 10 Operating System Support, see: https://kb.vmware.com/s/article/2150295

For Windows 10 Operating System Support, see: https://kb.vmware.com/s/article/2149393

APPENDIX F – MICROSOFT LICENSING RECOMMENDATIONS

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

The Service Offering does not provide any guest OS licensing required for the full use of the Service Offering. All necessary Microsoft licenses for operating Desktops and RDSH Servers are available from the customer's preferred Microsoft Licensing distributor.

For Horizon Cloud Service on IBM Cloud, Windows Server VMs used for either VDI desktops, RDSH servers or utility services must use Windows Server OS licenses. For VDI and RDSH workloads, customers are advised to bring one Windows Server Datacenter Edition for each host. In every standard (non vGPU) host cluster, there is one host reserved for High Availability, irrespective of how little the customer purchases. For customers planning to use only a few Windows Server VMs as utility services, please provide sufficient licensing (Standard or DC Edition) for a minimum of two hosts. Please consult with your VMware deployment services representative for complete details on the number of hosts and VMs that you are required to license from Microsoft.

Note: Since the Horizon Service and Microsoft's licensing policy may change over time, you must check with your VMware technical specialist for the latest recommendations.