Service Description

VMware vCloud® Air™

Last Updated: November 18, 2016

vmware®

The terms set forth in this Service Description apply to the VMware vCloud Air Service Offerings (each a "Service Offering" and collectively the "Service Offerings"). "VMware", "we" or "us" means VMware, Inc., a Delaware corporation, to the extent that you are purchasing a Service Offering in the United States, and VMware International Limited, a company organized and existing under the laws of Ireland, to the extent that you are purchasing a Service Offering elsewhere.

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

Contents

1.   Introduction

VMware vCloud® Air™ is a group of secure cloud service offerings operated by VMware, giving IT organizations a VMware-compatible platform to extend their cloud infrastructure and software deployments seamlessly beyond their data centers.

1.1   Self-Service Portals

The Service Offerings provide access to self-service consoles:

- **My VMware™ Account Management Console ("My VMware")** provides access to subscription status, and integrates navigation, viewing and management of all VMware product licenses and support under a single account.

- **VMware vCloud Air Console ("Console")** is the primary interface for access, consumption, and management of cloud resources purchased from VMware, including virtual data center management, and configuration of virtual machine instance lifecycle management on a per site basis. For more advanced management tasks, the Console provides direct access to vCloud Director.

- **VMware vCloud Air Networking Configuration Portal (for advanced networking services)** is the portal used for configuring advanced networking services features.

We will also provide organization administrator access to the vCloud® Application Programming Interface (API) for programmatic resource management or workload migration through vCloud Air Hybrid Cloud Manager.

1.2   Technical Documentation and Training

Documents and videos outlining key concepts with usage examples, a "Getting Started" guide, and "How To" guides for key objects are available through the vCloud Air Console. See also https://www.vmware.com/support.

1.3   Legal Terms

Use of the Service Offerings is subject to the Terms of Service at http://vcloud.vmware.com/legal.

1.4   Support

We will provide support for problems that you report to assist with adoption of and related to the Service Offerings. Support may be provided in any country in which we or our agents maintain facilities. To the extent you provide Your Content (as defined in the Terms of Service) in connection with support, we will handle Your Content in any such country in accordance with the Terms of Service.

2. vCloud Air IaaS Service Operations

Service Options

vCloud Air as an Infrastructure as a Service (IaaS) offering has five types of service:

- **Dedicated Cloud** provides a single-tenant private cloud with dedicated computing servers, layer-2 network isolation for workload traffic, dedicated storage volumes, and a dedicated cloud management instance. Infrastructure capacity may be allocated to a single virtual data center or to multiple data centers, at your option.

- **Virtual Private Cloud (VPC)** provides a multi-tenant virtual private cloud with logically-isolated resources on shared physical infrastructure, configured as a single virtual data center with networking resources.

- **Disaster Recovery on VPC** provides a reserved multi-tenant virtual private cloud, configured as a disaster recovery virtual data center (Disaster Recovery VDC) for replication, failover, and recovery of remote virtual machines. Similar to Virtual Private Cloud, this service leverages logically-isolated resources on shared physical infrastructure.

- **Dedicated Disaster Recovery** provides a reserved single-tenant private cloud, configured as a disaster recovery virtual data center (Dedicated VDC) for replication, failover and recovery of remote virtual machines. This service runs on the Dedicated Cloud service, providing dedicated computing servers, layer-2 network isolation for workload traffic, dedicated storage volumes, and a dedicated cloud management instance. Hybrid Cloud Manager (HCM) Advanced or Enterprise is required to enable the Disaster Recovery service.

- **Virtual Private Cloud OnDemand** provides a multi-tenant virtual private cloud with logically-isolated resources on shared physical infrastructure, allocated to a single virtual data center or to multiple virtual data centers, at your option.

Service Objects

Each type of service includes the capability to access these objects and manage them to align with different consumption and administration models:

- **Virtual Data Centers (VDCs)** in all types of service will be set up with an internal VDC network and edge gateway with optional NAT-routed network.

- **Virtual Machines (VMs)** are first-class objects in vCloud Air interactions; they may be created and managed individually. VMware vSphere® vApps™ will be visible along with their VM associations on the vCloud Air Console, but can be created or managed only through VMware® vCloud Director®.

- **Networks** may be managed through the vCloud Air network services console for edge gateway configuration and common use cases such as NAT mappings, firewall rules, and VM-to-network assignment. Advanced settings configuration and management such as VPN setup, load balancing, and network creation can be done through vCloud Director.

The following sections outline our respective roles and responsibilities in the delivery of the Service Offerings. While specific roles and responsibilities have also been identified as being owned by you, any roles or responsibilities not set forth in this Service Description are either not provided with the Service Offerings or are assumed to be your responsibility.

2.1 Service Provisioning

We will provide the following provisioning services:

- Implementation of platform components (physical servers, physical storage, and physical network devices) needed to support contracted resource pools when applicable.

- Providing initial network resources including default public IP addresses when applicable.

- Providing initial resource pools (memory, processing, primary storage, and networking) when applicable.

- Creating the initial administrative user account in the vCloud Air Console using default administrator privileges and system preferences.

You will be responsible for the following provisioning services:

- Creating user accounts in the vCloud Air Console, and changing default system preferences as needed.

- Creating and configuring applicable VDCs, vApps, VMs, and networks using deployment templates and wizards.

- Installing and configuring custom or third-party applications and operating systems on deployed VMs.

- Deploying and maintaining on-premises deployments of vSphere® Replication™ for use with Disaster Recovery, including but not limited to: installation of vSphere Replication, registering your local vSphere environment(s) with vCloud Air, selecting VMs for protection, and assigning a Recovery Point Objective (RPO) for replication frequency.

2.2 Data Recovery

We will provide the following services with respect to data recovery:

- Data protection, such as routine backups, for the vCloud Air infrastructure, including top-layer management and user-management interfaces owned and operated by us.

- Data and infrastructure restoration for the vCloud Air infrastructure, including top-layer management and user-management interfaces owned and operated by us.

You will be responsible for the following services with respect to data recovery:

- Data protection, such as routine backups, for the data and content accessed or stored on vCloud Air VMs or storage devices, configuration settings, etc.

- Data, content, VM, and configuration restorations for assets accessed or stored on your vCloud Air account.

2.3 Monitoring

We will provide the following services with respect to monitoring:

- Monitoring the vCloud Air infrastructure, infrastructure networks, top-layer management and user-management interfaces, and computing, storage, and network hardware for availability, capacity, and performance. We will also provide you with a VDC- and VM-level view of compute and storage resource utilization and availability.

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

- Monitoring the assets deployed or managed within your vCloud Air account, including but not limited to VMs, operating systems, applications, specific network configurations, operating system or application vulnerabilities, etc.

2.4 Incident and Problem Management

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

- Infrastructure over which we have direct administrative and/or physical access and control, such as vCloud Air servers, storage, and network devices.

- Service software over which we have direct administrative access and control, such as the vCloud Air Console, vCloud Director application, and other applications that we use in delivery of the Service Offerings.

- VMware-provided operating system templates, to the extent that
  - o Published templates cannot be accessed from the Service Catalog
  - o Published templates cannot be instantiated without modification
  - o Published templates cause errors at first run time
  - o There are substantial hangs or excessive delays in the retrieval of a template from the Service Catalog
  - o The configuration of a published template affects the VM's interaction with the hypervisor
  - o Time synchronization issues (NTP) exist

- VMware-provided tools, including
  - o VMware Tools installation and configuration
  - o VMware Tools optimization
  - o Performance tuning as it relates to VMware tools and drivers

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

- Your organization, VDC, vApp, or organization network administration, configuration, and modification.

- User-deployed and -configured assets such as VMs, custom developed or third-party applications, custom or user-deployed operating systems, network configuration settings, and user accounts.

- Operating system administration including the operating system itself or any features or components contained within it.

- Performance of user-deployed VMs, custom or third-party applications, your databases,

operating systems imported or customized by you, or other assets deployed and administered by you that are unrelated to the vCloud Air Console, vCloud Director, or the vCloud Air platform.

2.5 Change Management

We will provide the following change management elements:

- Processes and procedures to maintain the health and availability of the vCloud Air Console, the network services console, vCloud Director, or the vCloud Air platform.

- Processes and procedures to release new code versions, hot fixes, and service packs related to the vCloud Air Console, the network services console, vCloud Director, or the vCloud Air platform.

You are responsible for:

- Management of changes to your VMs, operating systems, custom or third-party applications, databases, and administration of general network changes within your control.

- Administration of self-service features provided through My VMware and the vCloud Air Console, up to the highest permission levels granted to you, including but not limited to VM and network functions, backup administration, user configuration and role management, general account management, etc.

2.6 Security

Responsibility for the end-to-end security of vCloud Air is shared between us and you. We will provide security for the aspects of the Service Offerings over which we have sole physical, logical, and administrative level control. You are responsible for the aspects of the Service Offerings over which you have administrative level access or control. The primary areas of responsibility as between us and you are set forth below.

We will use commercially reasonable efforts to provide:

- **Physical Security:** vCloud Air is housed in state of the art data center facilities. The following controls are in place at the physical layer in the vCloud Air data centers:

  o **Equipment Location:** VMware vCloud Air operates in the United States, EMEA and APAC. A site selection team determines each data center site. The site selection process includes a rigorous assessment, ensuring that each site has appropriate measures and countermeasures in place.

  o **Data Centers:** We use well-established data center providers to host workloads. Each data center is certified as a Tier 3 facility or higher. The providers are reviewed by independent third party auditors to meet the physical security requirements for ISO/IEC 27001 certification, SOC 1 Type 2/SSAE 16/ISAE 3401 and SOC 2 Type 2. Full AT101 reports outlining these specifications are available, upon request, subject to execution of an appropriate confidentiality and nondisclosure agreement.

- **Information Security:** We will protect the information systems used to deliver the Service Offerings for which we have sole administrative level control.

- **Network Security:** We will protect the networks containing our information systems up to the point where you have some control, permission, or access to modify the networks.

- **Security Monitoring:** We will monitor for security events involving the underlying infrastructure servers, storage, networks, and information systems used in the delivery of the Service Offerings 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 Offerings.

- **Patching and Vulnerability Management:** We will maintain the systems we use to deliver the Service Offerings, including the application of patches we deem critical for the target systems. We will perform routine vulnerability scans to surface critical risk areas for the systems we use to deliver the Service Offerings. Critical vulnerabilities will be addressed in a timely manner.

- **PCI Compliance:** If an environment is identified as PCI compliant, we will enforce Level 1 PCI compliance at the infrastructure level. This includes the security posture, patching, logging, and audit requirements for the vCloud Air IaaS offering (compute, network, and storage).

You are responsible for the following:

- **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 Offerings. 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 vCloud Air instance, associated with VMs, operating systems, applications, data or content surfaced through vulnerability scanning tools, or required for a compliance or certification program in which you are required to participate and which are not serviced under another VMware security program.

2.7   Virtual Server Deployment Templates

We will provide a catalog (the "Service Catalog") of supported virtual server deployment templates that you may deploy into your vCloud Air environments for Dedicated Cloud, Virtual Private Cloud, and Virtual Private Cloud OnDemand. The deployment and use of such templates will be subject to the Third Party Terms at http://vcloud.vmware.com/legal and may be subject to additional Subscription Software fees as further described in Appendix A of this Service Description. We will provide these templates, test them for quality, check for viruses, and install security patches before making them available in the Service Catalog. We will also maintain and update these templates from time to time. You are responsible for deploying and configuring the virtual server deployment templates that you choose to use, activating related licenses, and maintaining compliance with all applicable license terms.

In order to comply with our 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 Service Offerings, as set forth in the Third Party Terms. You may implement or import your own virtual server deployment templates so long as you have the legal right to deploy and use the software contained in such templates.

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

Note: Virtual server templates are not available in the Disaster Recovery service, since VDCs provisioned under that Service Offering are limited exclusively to replication of VMs from outside vCloud Air. You are responsible for ensuring that any VMs imported by way of replication, including third party software associated with those VMs, are in compliance with the applicable product use rights and license agreements.

2.8 Storage

vCloud Air includes persistent block storage as a part of the core subscription. There are two storage options available with a Dedicated Cloud, Virtual Private Cloud, or Virtual Private Cloud OnDemand instance: Standard Storage and SSD-Accelerated Storage. Disaster Recovery subscriptions do not have these two storage options. The two storage options allow for (1) growth of virtual machine disks (VMDKs) without downtime, and (2) the flexibility to migrate from one tier to the other as needed. You can also mix and match storage types per workload as needed.

By using a tiered storage approach with your vCloud Air instance, you can divide workloads in your environment according to performance requirements. For example, you can select SSD-Accelerated Storage for workloads requiring higher performance, or you can select Standard Storage for VMs that require lower performance (e.g., swap files). You can also dynamically blend storage types to best fit workload requirements. The core subscription for Dedicated Cloud includes 6TB of Standard Storage, and the core subscription for Virtual Private Cloud includes 2TB of Standard Storage. At the time of purchase, you can specify which type of storage should be included with your Service Offering instance. After the time of purchase, you can purchase more of the same storage option or the other option via My VMware or by submitting a purchase order to your reseller. All core component subscriptions are subject to service fees as further described in Appendix A of this Service Description. With Virtual Private Cloud OnDemand, you may dynamically choose your storage tier on a per-disk basis at the time of VM creation, and may change that storage tier at any point after VM creation.

A new high performance storage option is available only for the Dedicated Cloud offering. It is an all-SSD offering, that comes in two forms: (1) a 2TB high-performance storage SSD add-on that provides a maximum performance of 6,000 IOPS, and (2) a 2TB high-performance storage SSD add-on that provides a maximum performance of 12,000 IOPS.

2.9 Networking Services

The Service Offerings include the following network services as a part of the core Dedicated Cloud and Virtual Private Cloud subscription offerings:

- **Network Address Translation (NAT):** Separate controls for source and destination IP addresses, as well as port translation.
- **Dynamic Host Configuration Protocol (DHCP):** Configuration of IP pools, gateways, DNS servers, and search domains.
- **Firewall:** Supported rules include IP 5-tuple configuration with IP and port ranges for stateful inspection for all protocols.
- **Load Balancing:** Simple and dynamically configurable virtual IP addresses and server groups.
- **Site-to-Site Virtual Private Network (VPN):** Uses standardized IPsec protocol settings to interoperate with all major VPN vendors.
- **Static Routing:** Static routes for destination subnets or hosts.
- **Dynamic Routing:** Supported protocols include OSPF and BGP. This feature is available if you subscribe to the Direct Connect offering.
- **High Availability:** High availability ensures an active Edge on the network in case the primary Edge VM is unavailable.
- **Syslog Export:** Support for syslog export for all services to the remote servers.

You may also subscribe to optional add-ons -- Advanced Networking Standard or Advanced Networking Premium -- via My VMware. For both add-ons, you will have the following capabilities:

- **Distributed Firewall:** Distributed Firewall is a hypervisor kernel-embedded firewall that provides visibility and control for vCloud Air workloads and networks. It delivers close to line rate throughput to enable higher workload consolidation on physical servers. It is available only with a Dedicated Cloud Subscription that includes the Advanced Networking Standard or Advanced Networking Premium add-on.

- **SSL VPN-Plus:** SSL VPN-Plus enables remote users to connect securely to private networks behind an NSX Edge gateway.
- **Enhanced Load Balancing:** Application level load balancer.

- Advanced Networking Standard provides:
  - **High Capacity Site-to-Site Virtual Private Network (VPN):** 512 connections per edge gateway.
  - **High Capacity SSL VPN-Plus:** 50 users per edge gateway.

- Advanced Networking Premium provides:
  - **High Capacity Site-to-Site Virtual Private Network (VPN):** 1600 connections per edge gateway.
  - **High Capacity SSL VPN-Plus:** 100 users per edge gateway.

2.10 Migration

Migration of VMs, vApps and templates between vCloud Air and other vSphere or vCloud Director environments, such as data centers or vCloud Air evaluation environments, can be performed using vCloud Connector or vCloud Air Hybrid Cloud Manager. Export, transport, and import may use vCloud Connector or Open Virtual Machine Format (OVF); an optional Offline Data Transfer service is also available for migration to vCloud Air. These migration capabilities support onboarding to vCloud Air, export from vCloud Air, and synchronization of templates between vCloud Air and your on-premises data centers.

vCloud Connector supports migration of VMs, vApps, and templates between vCloud Air and other vSphere or vCloud Director environments, such as data centers or vCloud Air evaluation environments. In addition to the basic network-based copy operation of VMs, vApps, and templates between vSphere, vCloud Director, vCloud SP, and vCloud Air, vCloud Connector also supports the following use cases:

- Extend a single layer-2 network from your private vSphere and vCloud Director environments to vCloud Air so you can migrate VMs or vApps to vCloud Air while retaining the same IP and MAC address. This allows those VMs or vApps to communicate with other VMs or vApps in the private vSphere or vCloud Director environments.
- Synchronize your vCloud Air catalog with your private vSphere folder or vCloud Director catalog so that all authorized users of your private vSphere or vCloud Director and vCloud Air use the same templates.

2.11 Hybrid Cloud Manager (optional)

If you have a Dedicated Cloud subscription, vCloud Air Hybrid Cloud Manager offers a seamless option for extending your on-premises network to the cloud by creating an optimized, software-defined WAN to increase stretched network performance, enabling networks to stretch in the cloud yet perform almost as if they were local. Hybrid Cloud Manager also enables bi-directional migration of workloads as well as the migration of NSX security policies to vCloud Air Advanced Networking services.

With Hybrid Cloud Manager, you will have the following capabilities:
- Zero or low downtime migration between on-premises data center(s) and vCloud Air
- Accelerated migration for improved performance
- Network extension using vCloud Air's L2VPN-based extension feature, so you can stretch multiple L2 segments in one tunnel from on-premises vSphere environment(s) to vCloud Air, so VMs can migrate to vCloud Air while retaining the same IP and MAC address
- High performance network extension for increased network throughput over Direct Connect
- NSX distributed firewall policy migration – enables the Disaster Recovery Service for a Dedicated Cloud and allows all vSphere replication traffic through Hybrid Cloud Manager Cloud Gateway service for higher throughput performance.

You may subscribe to Hybrid Cloud Manager Standard, Hybrid Cloud Manager Advanced, or Hybrid Cloud Manager Enterprise via My VMware.

- Hybrid Cloud Manager Standard provides a 100 Mbps connection per vCenter Server
- Hybrid Cloud Manager Advanced provides a 1 Gbps connection per vCenter Server
- Hybrid Cloud Manager Enterprise provides a multi Gbps connection per vCenter Server

2.12 Offline Data Transfer Service (optional)

Offline Data Transfer ("ODT") is an optional data migration service for the purpose of transferring large numbers of VMs, vApps, or templates from your local private vSphere or vCloud Director environments to your vCloud Air environment. ODT may be procured through My VMware, and you will use vCloud Connector to invoke the service.

As part of this service, we will:

- Ship a physical storage device to you, permitting you to load VMs, vApps, or templates onto the device and ship it back to us using your preferred carrier. The content that you load onto the device will be encrypted by vCloud Connector. The decryption key is stored in the vCloud Air environment's vCloud Connector infrastructure, thereby ensuring security of your content during transfer.

- Transfer the data from the device into your vCloud Air instance.

You will be responsible for:

- Following the instructional documentation accompanying the storage device.

- Returning the storage device to us within 45 calendar days from date of shipment. If the storage device is not returned within the 45-day period, you will pay us a replacement fee for the storage device plus any shipping and handling charges, as assessed by us.

- Backing up any data, applications, or VMs transmitted via the service; we will not be responsible for any data loss that may occur as a result your use of this service.

This optional service may be subject to additional fees as further described in Appendix A of this Service Description.

2.13 vCloud Air vSphere Client Plug-in (optional)

The vCloud Air vSphere Client plug-in extends the familiar vSphere web client user interface to vCloud Air. With the vCloud Air plug-in, from within the vSphere client, you can:

- View and administer Dedicated Cloud and Virtual Private Cloud instances on vCloud Air.

- Browse, create, and modify each vCloud Air instance and manage its inventory of VDCs, gateways, and networks.

- Deploy VMs using catalog templates, and modify existing VMs.

- Receive automatic updates on any changes made to your account via the vCloud Air Console.

2.14 Data Protection (optional)

Data Protection is an optional service that provides secure, image-based backup and recovery capabilities that enable you to protect important VM data and content hosted in your vCloud Air environment. Through the Data Protection administration interface available in the vCloud Air Console, vApps and their VM members can be selected for policy-based backup and recovery operations.

Data Protection feature subscription and activation may be requested via My VMware and is subject to additional service fees based on the amount of backup data capacity. Backup data capacity for the service is measured in front end terabytes (FETB) and is described further in Appendix A of this Service Description. Once activated, vApps and their VM members may be registered and unregistered with Data Protection features on a self-service basis through the vCloud Air Console.

As part of this service, we will:

- Implement and maintain central service components (backup software appliances, backup and archival storage media and associated network topologies) needed to support Data Protection features.

- Perform routine configuration, maintenance, and optimization services on behalf of the Data Protection environment and in conformance with industry best practices.

- Allocate requisite backup storage based on capacity selections made at the time of subscription enrollment.

- Guarantee storage locality per geographical region for all backup data.

- Provide necessary Data Protection service reporting as requested.

You will be responsible for:

- Subscribing to Data Protection as an add-on feature via My VMware and selecting an amount of backup storage capacity commensurate with your requirements.

- Creating custom backup protection policies that may include, but are not limited to: affinity settings per VDC, scheduling, and retention periods.

- Registering and unregistering individual vApps and their VM members for scheduled backups using Data Protection.

- Performing any on-demand backups per vApp and its VM members.

- Performing in-place or out-of-place restores per vApp and/or individual VM.

- Managing any in-guest recovery tasks, including restore operations at the operating system, file systems and/or any application level.

- Managing backup storage capacity and consumption that may include, but is not limited to: activity reporting, ordering additional storage capacity via My VMware, and deleting any backup data in inventory to free up space.

2.15 Direct Connect (optional)

Direct Connect is an optional dedicated networking link that helps connect your remote data centers, and those in the same facility as vCloud Air, to your instances in vCloud Air environments. Direct Connect enables you to leverage high-throughput and low-latency connections provided by a network service provider. The dedicated connection circuit will consist of (1) the vCloud Air Direct Connect service (which is provided by us) and (2) the network connection and service from your site into the vCloud Air data center (which is provided by your chosen network service provider, who must have a point of presence in the relevant vCloud Air data center).

To enroll in Direct Connect you select, via My VMware, either a 10 Gbps or a 1 Gbps port speed for a vCloud Air Dedicated Cloud instance. For a Virtual Private Cloud instance and the Disaster Recovery service, only a 1 Gbps port is available.

The vCloud Air Direct Connect service is available in two versions:

- Direct Connect with Cross Connect: available in all vCloud Air data centers.

- Direct Connect for Network Exchange: available in select vCloud Air data centers. This version allows for faster provisioning of the service and connection redundancy when used with validated partners.

Your Direct Connect subscription will only include the port connection service from your chosen network service provider's point of presence in the vCloud Air data center to your vCloud Air instance.

Your network service provider will provide networking services and will assess fees (for which you are responsible) under separate service contract terms. These separate fees and terms are separate from your relationship with us.

As part of this service, we will:

- Provide either a 10 Gbps or 1 Gbps connection into vCloud Air, to which a customer-contracted circuit or connection can be linked.

- Provision, manage, and support the vCloud Air side of the connection.

- Coordinate with your selected network service provider to ensure successful circuit provisioning and connection from your vCloud Air instance to the network service provider's point of presence in the relevant vCloud Air data center(s).

You will be responsible for:

- Contracting with a network service provider for all private network service connectivity.

- Complying with all applicable terms and conditions of the network service provider.

- Providing all applicable network service provider circuit information to vCloud Air that is required for provisioning completion.

We will not be responsible for any network connectivity outage that occurs on the network service provider's side of the connection. Our Data Privacy Addendum applies to data processed on the vCloud Air infrastructure controlled by us, but not to the network connection and service provided by your chosen network service provider.

2.16 Disaster Recovery Multi-Tenant Solution (DRaaS VPC) (optional)

Disaster Recovery is an optional Recovery as a Service (RaaS) solution that provides protection for on-premises VMs hosted in vSphere environments. Disaster Recovery replicates those workloads to vCloud Air, and allows for self-directed failover and recovery in the cloud in the event of a disaster or similar disruptive event.

The Disaster Recovery service is comprised of both an on-premises software component and a cloud standby capacity component; the on-premises software component is vSphere Replication, and the cloud standby capacity component is a Disaster Recovery-VDC instance.

A Disaster Recovery-VPC instance is a virtualized recovery target in vCloud Air that includes a pre-configured mix of bandwidth, compute, network, and storage resources, which are reserved for test, failover, and recovery operations available exclusively in the Disaster Recovery Service Offering. These resource reservations are subject to the following limitations on service usage:

- Lease runtime for test failovers that exceeds 7 consecutive calendar days will incur Daily Usage Fees
- Lease runtime for live failover and recovery that exceeds 30 consecutive calendar days will incur Daily Usage Fees

As a part of this Service Offering, you may implement an unlimited quantity of test failover exercises. The Disaster Recovery Service Offering may be ordered as a core component using similar subscription enrollment methods as available for Dedicated Cloud and Virtual Private Cloud. Additional services specific to Disaster Recovery may also be added at the time of initial purchase or at any time during the

subscription term via My VMware. The Service Offering subscription components for Disaster Recovery are subject to additional service fees and are described in Appendix A of this Service Description.

As part of this Service Offering, we will:

- Provide secure remote access to reserved capacity for test, failover, and recovery operations based on the capacity quantities selected at the time of subscription enrollment and any additional quantity purchased up until the time a disaster is declared.

- Perform routine configuration, maintenance, and optimization services on behalf of the Disaster Recovery service environment and in conformance with industry best practices.

- Maintain versions of vSphere Replication appliance software as required by the Disaster Recovery service.

- Ensuring timely recovery of replicated VMs when you invoke a test or failover service request.

You will be responsible for:

- Enrolling in Disaster Recovery as a core subscription and selecting an amount of reserved capacity for Disaster Recovery that is commensurate with your requirements.

- Deploying vSphere Replication appliance software within your on-premises vSphere environment as necessary to support Disaster Recovery service functionality.

- Registering your on-premises vSphere environment with your designated Disaster Recovery-VDC instance in vCloud Air.

- Ensuring the appropriate network connectivity type and bandwidth is available between your on-premises environment and vCloud Air to support your replication requirements.

- Configuring VMs for protection in the Disaster Recovery service, and defining a corresponding RPO per VM.

- Developing any custom runbook procedures for test, failover, recovery, and failback operations available as part of the Disaster Recovery service.

- Implementing and executing any recovery tasks that extend beyond the scope of Disaster Recovery and the recovery of VMs as the prime service boundary.

- Ensuring sufficient reserved capacity is available in your Disaster Recovery-VDC instance to accommodate variable failover loads.

2.17 Object Storage (optional)

VMware vCloud Air Object Storage is an optional service that provides a scalable, cost-effective, and resilient cloud-based storage solution for unstructured data. The service allows customers to gain instant self-service access to storage capacity, on demand, and to scale up to petabytes.

Currently, there is one service in the vCloud Air Object Storage portfolio:

- **VMware vCloud Air Object Storage powered by Google Cloud Platform:** Within this service, you have three options for storage:

  o Standard storage – for workloads that require high levels of performance, availability and durability,

  o Durable Reduced Availability storage – for workloads that can run on lower levels of performance and availability but which require high durability, and

  o Nearline storage – for long-term storage of infrequently accessed data that requires lower levels of performance and availability relative to the other two offerings.

Object Storage powered by Google Cloud Platform is a vCloud Air OnDemand service running on Google Cloud Storage. Its services leverage the billing and metering, and identity and access management components of the vCloud Air OnDemand platform. Its services are available under the VMware vCloud Air Terms of Service, and are fully supported by VMware's Global Shared Services team.

VMware vCloud Air Object Storage feature subscription and activation may be requested via My VMware, and is subject to additional service fees based on the amount of storage, network egress, and transactions. Storage, network egress, and transactions are described further in Appendix A of this Service Description. Once activated, vApps and their VM members may be registered and unregistered with Object Storage features on a self-service basis through the vCloud Air Console.

As part of this Service Offering, we will:

- Implement and maintain all central service components (such as billing and metering, and identity and access management) needed to support Object Storage features.
- Allow access to object storage platforms hosted by Google.
- Perform routine configuration, maintenance, and optimization services on behalf of the Object Storage service components hosted on vCloud Air. We also will work with Google to perform these same routine services on the services hosted by that platform. All of these activities will be performed in conformance with industry best practices.
- Allocate requisite object storage capacity based on your requests for the appropriate type of storage.
- Guarantee storage locality per geographical region selected for all object storage data.

You will be responsible for:

- Subscribing to Object Storage powered by Google, as an add-on feature, via My VMware.
- Creating and maintaining service accounts and p12 certificates for Object Storage powered by Google.
- Sharing access keys and certificates with individual vApps and their VM members for using Object Storage.
- Creating and managing buckets and objects on Object Storage.
- Managing Object Storage capacity and consumption that may include but is not limited to activity reporting, and managing creation and deletion of buckets and objects.
- Upon termination of your vCloud Air account, deleting the associated buckets and objects in order to prevent being billed for the buckets and objects created by you.
- Submitting any billing claims within 60 days of the issuance of the bill.

2.18   Dedicated Disaster Recovery (optional)

Dedicated Disaster Recovery is an optional Recovery-as-a-Service (RaaS) solution that provides protection for on-premises VMs hosted in private vSphere environments. Disaster Recovery replicates those workloads to vCloud Air and allows for self-directed failover and recovery in the cloud in the event of a disaster or similar disruptive event.

The Dedicated Disaster Recovery service is comprised of both an on-premises software component and a cloud standby capacity component: the on-premises software components are Hybrid Cloud Manager with vSphere Replication; and the cloud standby capacity component is a Dedicated-VDC instance. More than one VDC can be created and used as a DR target for vSphere Replication.

vSphere Replication is our proprietary replication engine that operates at the hypervisor level. It enables protection of individual VMs and their associated virtual machine disk(s) (VMDK). Your use of vSphere Replication is subject to the terms of the End User License Agreement for vSphere Replication.

Hybrid Cloud Manager creates an optimized, software-defined WAN to increase stretched network performance. Hybrid Cloud Manager also enables bi-directional migration of workloads as well as the migration of NSX security policies to vCloud Air Advanced Networking services.

A Dedicated-VDC instance is a virtualized recovery target in vCloud Air which is reserved for test, failover, and recovery operations available exclusively in the Dedicated Disaster Recovery Service Offering.

As a part of this Service Offering, you may implement an unlimited quantity of test failover exercises. The Dedicated Disaster Recovery Service Offering may be ordered with a Dedicated Cloud and adding Hybrid Cloud Manager to your subscription.

As part of this Service Offering, we will:

- Provide secure, remote access to reserved capacity for test, failover, and recovery operations based on the capacity quantities selected at the time of subscription enrollment and any additional quantity purchased up until the time a disaster is declared.

- Perform routine configuration, maintenance, and optimization services on behalf of the Disaster Recovery service environment in conformance with industry best practices.

- Maintain versions of vSphere Replication and Hybrid Cloud Manager appliance software as required by the Dedicated Disaster Recovery service.

- Ensuring timely recovery of replicated virtual machines if you invoke a test or failover service request,

You will be responsible for:

- Subscribing to Dedicated Cloud with Hybrid Cloud Manager as a core subscription and selecting an amount of reserved capacity for Disaster Recovery that is commensurate with your requirements

- Deploying vSphere Replication and Hybrid Cloud Manager appliance software within your on-premises vSphere environment as necessary to support Disaster Recovery service functionality

- Registering Hybrid Cloud Manager with a Dedicated-VDC instance in vCloud Air and deploying Hybrid Cloud Manager.

- Registering your local vSphere environment with your designated Dedicated-VDC instance in vCloud Air.
- Ensuring the appropriate network connectivity type and bandwidth is available between your on-premises environment and vCloud Air to support your replication requirements.
- Configuring VMs for protection in the Dedicated Disaster Recovery service and defining a corresponding RPO per VM.
- Developing any custom runbook procedures for test, failover, recovery, and failback operations available as part of the Dedicated Disaster Recovery service.
- Implementing and executing any recovery tasks that extend beyond the scope of Disaster Recovery and the recovery of VMs as the prime service boundary.
- Ensuring sufficient reserved capacity is available in your Dedicated-VDC instance to accommodate variable failover loads.

3. Business Operations

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

3.1 Ordering and Invoicing

Dedicated Cloud, Virtual Private Cloud, and Disaster Recovery Ordering

- Initial orders include core Compute, Support, Storage, IP Address, and Internet Bandwidth components for a single Service Offering instance ("Service Identifier" or "SID") and are described in further detail in Appendix A. The initial purchase establishes the default billing relationship that applies to all transactions for that SID for the duration of the contract; for example, if your initial vCloud Air order is placed through a VMware authorized reseller, then subsequent payments related to your Service Identifier will be made through that reseller. This billing relationship may be modified at the time of subscription renewal.

- Additional capacity may be purchased at the time of your initial order or any time after the initial order.

- Additional services, such as Data Protection, may be purchased with the initial order or through My VMware at any time during the subscription term. Additional terms and fees may apply to such additional services.

- Account changes to capacity may be made by ordering additional capacity or services any time before the end of the subscription term.

- Changes to the VMware authorized reseller associated with your SID may be made at the time of subscription renewal, by contacting us.

- Service reductions may be coordinated with us at the time of subscription renewal and will require a new order for the reduced Service Offering capacity. However, if the capacity associated with your reduced Service Offering order is less than the capacity required to sustain your then-current workloads, we will bill you for the excess capacity at the then-current rates until such time as you have released the excess capacity and we have reclaimed it.

Virtual Private Cloud OnDemand Ordering

- Initial sign-up includes the provisioning of a single SID once the payment method is provided and authorized. Sign-up provides entitlement to consume any OnDemand service components available from time to time, but does not provision any of those service components by default.

- Initial and additional capacity may be allocated from within the Service Offering any time after the initial sign-up.

- Additional services, such as Offline Data Transfer, may be purchased through My VMware at any time during the Billing Period. Additional terms and fees may apply to such additional services.

- Account changes to capacity may be made by allocating or ordering additional capacity or services any time before the end of the Billing Period.

- Service reductions may be made from within the Service Offering at any time during the Billing Period.

Dedicated Cloud, Virtual Private Cloud, and Disaster Recovery Invoicing

- When you purchase any of the above Service Offerings directly from us, we will invoice you for all ordered services within thirty (30) business days after the beginning of each Billing Period. When you purchase any of the above Service Offerings through a VMware authorized reseller, the reseller will invoice you as mutually agreed between you and that reseller.

- Plan Charges, as defined in Appendix A to this Service Description, will be invoiced by us for the then-current Billing Period unless you choose a prepaid Service Offering SKU, in which case you will be billed for the ordered subscription term. If the Service Offering is not provided for the entire Billing Period, then the fees for such period will be prorated (a) from the day the Service Offering was first provided through the end of the Billing Period, or (b) from the beginning of the Billing Period through the last day in the Billing Period on which the Service Offering was provided, as appropriate.

- Usage Charges, as defined in Appendix A to this Service Description, will be invoiced by us on the next billing date following the Billing Period in which they were incurred. If your SID is provisioned within 5 business days after the Billing Date, you may not receive the first invoice for Usage Charges until the second Billing Date following your SID provisioning.

Virtual Private Cloud OnDemand Invoicing

- For any OnDemand Service Offerings, we will invoice you for all consumed services within 30 business days after the beginning of each Billing Period. The amount you owe will be deducted from your Subscription Purchasing Program balance at the time of invoicing.

3.2 Metered Usage

Metered Usage Components for Dedicated Cloud, Virtual Private Cloud and Disaster Recovery, such as Bandwidth and third-party licenses, are available. You are obligated to pay for such Metered Usage Components at the then-current rates published by us if you purchased the Service Offering directly from us, or at the rates agreed with your VMware authorized reseller if you purchase the Service Offering through that reseller. Such charges will be billed as Usage Charges. A list of Metered Usage Components is provided in Appendix A to this Service Description.

Add-on capacity and services for Dedicated Cloud and Virtual Private Cloud as described above may be purchased at any time to meet new or expanded requirements.

- Capacity may be added via My VMware or through your preferred reseller.

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

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

The below DRaaS add-ons are not considered metered services. They are one-time purchase options for DRaaS use cases:

- One-time compute capacity (30 days) may be purchased to satisfy short-term failover capacity requirements that exceed the original amount of failover capacity designated at the time of initial subscription enrollment.
- If the one-time compute capacity add-on (30 days) is purchased but the underlying core subscription expires prior to the end of the 30-day period for the compute add-on, the compute add-on will terminate at the same time as the core subscription expiration, unless the core subscription is renewed.
- One-time compute capacity may be purchased as often as required to support live failover and recovery operations throughout the subscription term.
- Usage entitlement for one-time compute capacity will remain in effect until the 30-day expiration is reached, and is independent of any Runtime Leases associated with the core capacity – the latter of which is applied at the time of an actual test failover or live failover and recovery event.

All Virtual Private Cloud OnDemand components are considered metered usage.

3.3 Renewal

Dedicated Cloud, Virtual Private Cloud, and Disaster Recovery

We reserve the right to not renew a 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 3.3, each SID will automatically renew using the current configuration and subscription term duration. The SKUs and pricing, based on the applicable price list at the time of renewal, will be applied to the renewal term. You may opt out of auto-renewal by changing your renewal method setting to "Modify" or "Cancel" for the SID within My VMware.

Modify at End of Subscription Term

When you select the renewal method setting "Modify", you will be contacted prior to the end of the SID 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, for the renewal subscription term by issuing a new purchase order. If you do not make any changes to your current SID, and/or you do not issue a new purchase order for the new Service Offering to us or to your VMware authorized reseller (if applicable), by the applicable deadline specified below, then your existing SID, as currently configured, will automatically renew. If you purchase a Service Offering through a VMware authorized reseller, a manual renewal is the only time you may elect a change in reseller relationship for that specific SID. See the table below for the deadlines to manage your manual renewal.

Subscription Term	Deadline to Submit Modified Renewal Order
Less than or equal to 3 months	The renewal method in My VMware must be set to "Modify" and your purchase order for the modified configuration must be received by us at least 5 business days before the end of the subscription term. Please allow processing time for you and/or your authorized reseller to meet this deadline.
More than 3 months	The renewal method in My VMware must be set to "Modify" and your purchase order for the modified configuration must be received by us at least 30 business days before the end of the subscription term. Please allow processing time for you and/or your authorized reseller to meet this deadline.

Cancel at End of Subscription Term

You may cancel your existing SID renewal by changing your renewal method setting for the SID within My VMware to "Cancel". When this option is set, your access to all Service Offerings for the SID will expire at the end of the SID subscription term. Please see the table below for the deadlines to select the cancel option via the My VMware portal.

Subscription Term	Deadline to Select Cancel Option via My VMware
Less than or equal to 3 months	5 business days prior to the last day of the current SID subscription term
More than 3 months	30 business days prior to the last day of the current SID subscription term

<u>**Virtual Private Cloud OnDemand**</u>

We reserve the right to not renew a SID at the end of its Billing Period, in which case we will notify you prior to the end of the Billing Period. Renewal options for each SID may be selected using the My VMware portal.

Auto-Renewal (the default setting)

Except as set forth in this Section 3.3, each SID will automatically renew using the current configuration, for 30 days. The then-current pricing at the time of renewal will be applied to the renewal term. You may opt out of auto-renewal by cancelling the Service Offering prior to the next Billing Period within My VMware. If you choose to cancel the Service Offering, your cloud environment (i.e., your SID) will be terminated. VMs and storage will be deleted, and the resources will be reclaimed.

Cancellation

You may terminate your existing SID at any time prior to the next Billing Period by cancelling the Service Offering within My VMware. When this option is selected, your access to the Service Offering will expire immediately. You will be charged a cancellation fee for terminating your subscription prior to the end of the subscription term.

3.4 Suspension and Re-Enablement

- During the time a SID is **suspended** for delinquent payment or any other reason as set forth in the Terms of Service, we will restrict access to all SIDs and block all traffic across their public IP Addresses. We will retain SIDs with configurations and data intact until the issue is resolved or the Service Offering subscription expires or is terminated.

- **SID re-enablement** will be initiated immediately upon resolution of the account issues that led to suspension; access to the Service Offering(s) and traffic across IP Addresses will be restored.

3.5 Termination

- Full termination of an SID due to contract expiration, termination, cancellation, or any other cause will result in permanent loss of access to the environments, discontinuation of services, and a deletion of such environments, configurations, and data according to applicable VMware policies.

- Data from a terminated SID will be retained by us for 90 days following termination of such SID. We will delete the data after this 90-day period.

- For Disaster Recovery SIDs that have ended due to contract expiration, termination, cancellation, or any other cause prior to test and/or failover Runtime Leases having fully expired, the end of the subscription will result in immediate forfeiture of any Runtime Lease balances for test or failover operations.

3.6   Early Termination (Dedicated Cloud, Virtual Private Cloud, and Disaster Recovery Only)

vCloud Air monthly-paid subscriptions with an initial term of 12 months or more are eligible for early termination. Prepaid subscriptions are not eligible for early termination. Add-on services are eligible for early termination only to the extent that the underlying monthly-paid subscription is also terminated. The termination can be effective only after the first 3 months of the subscription term, and with advance notice to us. You also must pay a fee equal to one month of contracted subscription fees (including add-on fees) for every 12-month period (or portion thereof) remaining on the subscription term as of the effective termination date. For example:

Months Remaining on Subscription Term at Effective Termination Date	Early Termination Fee Amount
Less than 12 months	Equal to 1 month of remaining contracted subscription fees (including add-on fees)
At least 12 months, but less than 24 months	Equal to 2 months of remaining contracted subscription fees (including add-on fees)
At least 24 months, but less than 36 months	Equal to 3 months of remaining contracted subscription fees (including add-on fees)

To give the required notice for the SID you want to terminate, please contact the VMware Global Support and Services team by filing a support request through the My VMware portal.

You must provide 30 days' advance notice to us. The termination (the last active day for your SID) will be the last day of your next Billing Period.

- For example, if your subscription Billing Period ends on the 15th of each month (please note that this may be different from your Billing Date), you must notify us by April 15th to terminate your SID effective May 15th; if notice is provided on April 16th, the SID will be terminated effective June 15th.

Note: Monthly-paid subscriptions for Disaster Recovery are eligible for the early termination option described above. However, the fee associated with an early termination for Disaster Recovery will be waived IF: (1) you upgrade from Disaster Recovery to either Dedicated Cloud or Virtual Private Cloud in the same Billing Period when you cancel your Disaster Recovery service subscription, and (2) you also purchase a new service subscription for either Dedicated Cloud or Virtual Private Cloud for a subscription term equal to or greater than your original Disaster Recovery subscription term.

Appendix A – Ordering and Metered Usage Components

This Appendix A describes the components that may be purchased by the customer via initial or subsequent orders, and components that will be billed based on actual usage.

Definitions:

"Bandwidth" is the network connectivity from your vCloud Air environment to the public Internet using our Internet service providers. Bandwidth is consumed when data is either transferred or received by your Service Offering instance.

"Billing Date" is the date when we will bill for the Service Offering. Billing Dates will occur monthly, unless otherwise noted.

"Billing Period" is the period for which the Service Offering is being billed. Billing Periods are monthly and are related to the provisioning of your SID, unless otherwise stated.

"Burst Bandwidth" is the amount of Bandwidth consumed by you in excess of the Bandwidth purchased with your Core Components for Dedicated Cloud, Virtual Private Cloud, and Disaster Recovery.

"Compute" is the allocated virtual processing and virtual memory resources available to you through your purchased Service Offering. Compute is ordered in the increments set forth below for Dedicated Cloud, Virtual Private Cloud, and Disaster Recovery.

"Core Components" are Compute, Storage, Bandwidth, IP Addresses, and Support for Dedicated Cloud, Virtual Private Cloud, and Disaster Recovery.

"Daily Usage Fee" is the extra cost associated with operating any VMs that have been failed over or recovered through the Disaster Recovery Service Offering for longer than the allowed Runtime Lease.

"Elastic Compute" is the unreserved virtual processing and virtual memory resources utilized by you during a Billing Period for Dedicated Cloud, Virtual Private Cloud, and Disaster Recovery.

"Failover Test" is the act of performing a simulated failover and recovery exercise as part of Disaster Recovery, and applies whenever one or more VMs is included in the test workflow.

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

"Metered Usage Components" are those Service Offering elements that are billed based upon actual usage, including any usage in excess of the committed Plan Charges. Metered Usage Components are listed below.

"Offline Data Transfer" is a data migration service where a physical storage device is shipped to you and then returned to us for the purpose of transferring large numbers of VMs, vApps, or templates from your local VMware vSphere or VMware vCloud Director environment to your vCloud Air environment.

"Plan Charges" are those Service Offering components that are not billed based upon usage (i.e., those components that you have committed to purchase and that are recurring during the subscription term without regard to use). These charges will be invoiced for the then-current Billing Period as described in Section 3.1 of the Service Description.

"Runtime Lease" is the amount of time (measured in days) that a VM can be operational as part of Disaster Recovery.

"Storage" contains block level storage volumes made available to you through your purchased Service Offering. Storage is ordered in the increments set forth below or is allocated from within the Service Offering.

"Subscription Software" is any software provided to you and for which you are billed for its use.

"Support" is the service delivered by VMware as set forth at https://www.vmware.com/support/vcloud-air-html.

"Third-Party Licenses" are those licenses for third-party software that are made available to you as optional services (either through the Service Catalog or otherwise).

"UOM" is the Unit of Measure for measuring usage for billing purposes.

"Usage Charges" are the service fees for those Service Offering components that are billed based upon usage. These charges will be invoiced as described in Section 3.1 of the Service Description.

Ordering vCloud Air IaaS Subscription Core Components

Subscription core components for Dedicated Cloud, Dedicated Disaster Recovery, Virtual Private Cloud, and Disaster Recovery are ordered for specific subscription terms (i.e., monthly, or in 3, 12, 24, or 36 month periods). Each component will be invoiced and payable on a monthly basis, or invoiced and payable as a lump sum if a prepaid subscription is purchased. Refer to the support URL referenced above for details on required support.

Dedicated Cloud

For Dedicated Cloud, in each initial order for a SID instance, you must include a Dedicated Cloud Core which is comprised of the following components:

- Compute: 35Ghz vCPU and 240GB of vRAM
- Storage: 6TB
  o Standard Storage or SSD-Accelerated Storage
- Bandwidth: 50Mbps
- IP Addresses: 3 Public IP Addresses
- Support: 24x7 Production Support

Add-on capacity can be used to increase overall SID capacity; it must be ordered in the following whole increments:

- Compute: 35Ghz vCPU and 240GB vRAM
- Storage: 6TB
  o Standard Storage or SSD-Accelerated Storage
- Bandwidth: 50Mbps
- IP Addresses: 1 Public IP Address
- Support: 24x7 Production Support

Note: The above capacity amounts may not be available in all regions, in which case the above items must be ordered in the capacity increments available in the respective region.

Dedicated Disaster Recovery Cloud

For Dedicated Disaster Recovery Cloud instances, in each initial order for a SID instance, you must include a Dedicated Cloud core which is comprised of the following components:

- Compute: 35Ghz vCPU and 240GB of vRAM
- Storage: 6TB_
  ▪ Standard Storage or SSD-Accelerated Storage or High Performance Storage

- Bandwidth: 50Mbps
- IP Addresses: 3 Public IP Addresses
- Support: 24x7 Production Support

The following components are required to enable the Disaster Recovery service:

- 2 additional Public IP addresses
- Hybrid Cloud Manager Advanced or Enterprise edition

Add-on capacity can be used to increase overall DR reserved capacity and must be ordered in the following whole increments:

- Compute: 35Ghz vCPU and 240GB vRAM
- Storage: 6TB
- Standard Storage or SSD-Accelerated Storage or High Performance Storage
- Bandwidth: 50Mbps
- IP Addresses: 1 Public IP Address
- Support: 24x7 Production Support

Note: The above capacity amounts may not be available in all regions, in which case the above items must be ordered in the capacity increments available in the respective region.

Virtual Private Cloud

For Virtual Private Cloud, in each initial order for a SID instance, you must include a Virtual Private Cloud Core which is comprised of the following components:

- Compute: 10Ghz vCPU and 20GB of vRAM
- Storage: 2TB
  - o Standard Storage or SSD-Accelerated Storage
- Bandwidth: 10Mbps
- IP Addresses: 2 Public IP Addresses
- Support: 24x7 Production Support

Add-on capacity can be used to increase overall SID capacity; it must be ordered in the following whole increments:

- Compute: 10GHz vCPU and 20GB vRAM
- Storage: 2TB
  - o Standard Storage or SSD-Accelerated Storage
- Bandwidth: 10Mbps
- IP Addresses: 1 Public IP Address
- Support: 24x7 Production Support

Note: The above capacity amounts may not be available in all regions, in which case the above items must be ordered in the capacity increments available in the respective region.

Disaster Recovery

For Disaster Recovery-VDC, in each initial order for a VDC instance, you must include a Disaster Recovery Core which is comprised of the following components:

- Compute: 10Ghz vCPU and 20GB of vRAM
- Storage: 1TB
- Bandwidth: 10Mbps
- IP Addresses: 2 Public IP Addresses
- Support: 24x7 Production Support

Add-on capacity can be used to increase overall VDC instance capacity; it must be ordered in the following whole increments:

- Compute: 10GHz vCPU and 20GB vRAM
- Storage: 1TB Standard Storage
- Bandwidth: 10Mbps
- IP Addresses: 1 Public IP Address
- Support: 24x7 Production Support

Note: The above capacity amounts may not be available in all regions, in which case the above items must be ordered in the capacity increments available in the respective region.

Metered Usage Components

Consumption of these components is measured based on the UOMs and increments described below. These components incur Usage Charges, and will be billed as described in Section 3 of the Service Description.

Pricing for these components will vary based upon your ordering path. See "Fees and Charges" below.

IaaS Service Offerings:

Dedicated Cloud, Virtual Private Cloud, and Disaster Recovery

- Burst Bandwidth
  - Consumption Interval: Billing Period
  - Increments: per 1Mbps

- Third-Party Licenses
  - Microsoft SPLA Subscription Software
    - Consumption Interval: Calendar month, or any portion thereof
    - Increments: per CPU

- Data Protection Storage Capacity
  - Consumption Interval: Billing Period
  - Increments: per front end terabyte (FETB) of data protected

- Daily Usage Fee for Compute Capacity in Disaster Recovery
  - Consumption Interval: Calendar month, or any portion thereof
  - Increments: per number of days that reserved CPU and memory capacity is online and in use in excess of the allotted Runtime Lease periods

- Failover Test Credits for Disaster Recovery
  - Consumption Interval: 12-month period (calculated using the monthly Billing Date as the start of each Billing Period)
  - Increments: per Failover Test event
  - Limitations: additional Failover Test credits must be used within the same 12-month period as the core Disaster Recovery subscription. After 12 months, all tests associated with the Disaster Recovery SID will expire/be reset (depending on subscription term length).

Virtual Private Cloud OnDemand

- vCPU
  - Consumption Interval: Minute/Billing Period
  - Increments: GHz

- vRAM
  - Consumption Interval: Minute/Billing Period
  - Increments: GB

- Standard Storage
  - Consumption Interval: Minute/Billing Period
  - Increments: GB/Month

- SSD-Accelerated Storage
  - Consumption Interval: Minute/Billing Period
  - Increments: GB/Month

- Bandwidth
  - Consumption Interval: Billing Period
  - Increments: MB

- Public IP Address
  - Consumption Interval: Minute/Billing Period
  - Increments: per Public IP Address

- Third-Party Licenses
  - Microsoft SPLA Subscription Software
    - Consumption Interval: Minute/Billing Period
    - Increments: per CPU

- Support
  - Provides 24x7 production support as an additional paid service
  - Consumption Interval: Billing Period
  - Increments: Support is charged as a percentage of total invoice amount

Object Storage powered by Google Cloud Platform

- Storage Capacity:
  - Consumption Interval: Per-second billing; billing data refreshed every day
  - Increments: GB/Month

- Nearline Storage Reads: Charge for reading data stored as Nearline Storage
  - Consumption Interval: Per-second billing; billing data refreshed every day
  - Increments: GB read

- Nearline Early Deletion: Charge for deleting data stored as Nearline Storage before 30 days
  - Consumption Interval: Per-second billing; billing data refreshed every day
  - Increments: GB

- Egress: Outbound data transfer from vCloud Air Object Storage powered by Google Cloud Platform to the Internet
  - Consumption Interval: Per-second billing; billing data refreshed every day
  - Increments: GB

- Inter-region Egress and Ingress: Date transferred amongst NA, EU and APAC regions in vCloud Air Object Storage powered by Google Cloud Platform
  - Consumption Interval: Per-second billing; billing data refreshed every day
  - Increments: GB

- Class A Operations: Special category inbound and outbound operations as defined at https://cloud.google.com/pricing/cloud-storage
  - Consumption Interval: Per-second billing; billing data refreshed every day
  - Increments: 1,000 operations

- Class B Operations: Special category inbound and outbound operations as defined at https://cloud.google.com/pricing/cloud-storage
  - Consumption Interval: Per-second billing; billing data refreshed every day
  - Increments: 10,000 operations

One-Time Components

The one-time components listed below may be ordered. Each of these components is more fully described in the Service Description:

- Offline Data Transfer: A single physical data transfer up to 11TB

Pricing for these components will vary based upon your ordering path. Please see "Fees and Charges" below.

Fees and Charges

When you order directly from us, we will invoice you based upon the fees listed in our then-current applicable price list, or as otherwise agreed in the order. When you order from a VMware authorized reseller, that reseller will invoice you based upon its price list or as otherwise agreed with you.

Orders that add services or capacity to an existing SID may be direct with us or placed with a reseller, depending on how the original SID was placed. The subscription term(s) for such additional services or capacity will be coterminous with the end of the SID subscription period. That is, if a reseller is already billing you for the SID, then the order for such additional services or capacity will also be placed through that reseller, and the price that you agree to pay and other applicable terms will be as agreed with that reseller.