NOTICE: This Service Description is no longer being updated. Content has been moved to the Cloud Services Guide, found at https://www.vmware.com/agreements

Service Description

VMware Cloud™ on AWS

Last updated: 29 August 2022

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, and 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. All terms used but not defined in this Service Description are defined in the Terms of Service or other documents comprising the Agreement between you and us regarding your use of the Service Offering.

The VMware Privacy Notices describe how personal information may be collected, used, shared, or otherwise processed by VMware as a data controller. The VMware Privacy Notices are available at https://www.vmware.com/help/privacy.html.

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

Introduction

VMware Cloud™ on AWS (the "Service Offering" or "VMware Cloud") brings VMware's enterprise class software defined data center offering to the Amazon Web Services cloud, enabling customers to run any application across vSphere-based private, public, and hybrid cloud environments.

The Service Offering has the following components:

- Software Defined Data Center ("SDDC") consisting of:
  - VMware vSphere® running on elastic bare metal hosts deployed in AWS
  - VMware vCenter Server® appliance
  - VMware NSX® Data Center to power networking for the Service Offering
  - VMware vSAN™ aggregating host-based storage into a shared datastore
  - VMware HCX® enabling app mobility and infrastructure hybridity
- Self-service provisioning of SDDCs, on demand, from vmc.vmware.com
- Maintenance, patching, and upgrades of the SDDC, performed by VMware

Service Consoles

The Service Offering includes access to the following consoles:

- VMware Cloud Console (the "VMC Console") is the primary user interface for provisioning SDDCs.
- VMware Cloud Services Discovery Console provides a common entry point for many VMware cloud service offerings, including the Service Offering.
- VMware vSphere® client (in the customer SDDC) provides access to manage workloads and the compute, storage, and network components of the SDDC.
- VMware Cloud status page (status.vmware-services.io) for communicating the status of the Service Offering.

Additional Information and Applicable Legal Terms

Technical Documentation and Training

Documents outlining Key Concepts with usage examples, a "Getting Started" guide, and "How To" guides for key features are available at https://docs.vmware.com/vmc.

Legal Terms

Use of the Service Offering is subject to the VMware Cloud Service Offerings Terms of Service ("Terms of Service"), available through a link on the main VMware end user terms landing page: https://www.vmware.com/download/eula.html.

Service Operations Data

In connection with providing the Service Offering, VMware collects and processes information from VMware's software or systems hosting the Service Offering, and from the customer's systems, applications, and devices that are used with the Service Offering, such as configuration, performance, and log data. This information is processed to facilitate delivery of the Service Offering, including but not limited to (i) tracking entitlements, (ii) providing support, (iii) monitoring and ensuring the performance, integrity, and stability of the Service Offering's infrastructure, and (iv) preventing or addressing service or technical issues. To the extent any of this data is

considered personal data under applicable data protection laws, the data will be treated in accordance with VMware's Privacy Notice, including the VMware Products and Services Notice available at: https://www.vmware.com/help/privacy.html.

Usage Data

The Service Offering collects data directly from VMware's software or systems hosting the Service Offering, and from the customer's systems, applications, and devices involved in the use of the Service Offering, such as configuration, performance, and usage data, to improve VMware products and services, and your and your users' experience, as more specifically described in VMware's Trust and Assurance Center, 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 Notices available at https://www.vmware.com/ help/privacy.html. More information on how to choose whether to accept certain cookies used by VMware websites and solutions can also be found from that link.

Data Retention and Deletion

Retention and storage policies associated with Your Content (including any personal data stored within Your Content) are solely managed by you. VMware does not back up Your Content and therefore will not be able to recover any of Your Content in any unforeseen event.

You are responsible for implementing tools, products, and operational procedures to support data migration, data protection, backup/archive, and restoration for all of Your Content and all configurations created by you in the SDDC, including Virtual Machines and Content Libraries.

Termination of your Service Offering instance will result in permanent loss of access to the environments, discontinuation of services, and a deletion of the environments and configurations pursuant to VMware practices. Any deletion of a host on VMC results in an automated cryptographic wipe of the hard drive is performed via destruction of keys used by the self-encrypting drives. This cryptographic erasure ensures that there is no Customer Content on the drives before returning the servers to the pool of available hardware to be reprovisioned or decommissioned from service.

Service Operations Data and Usage Data is backed up by VMware. A storage policy enforces retention of three years and automatically purges log events that exceed the three-year lifecycle.

Use of FullStory

The Service Offering uses FullStory functionality to collect data directly from any browsers used to access and use the Service Offering. FullStory collects data regarding your use of the Service Offering, including user interaction and behavior, to enable session replay. The data collected and inferred is used by VMware to diagnose and improve its products and services, and to address issues.

For users who wish to opt out of session recording, FullStory makes the following website available: https://www.fullstory.com/optout/.

Use of Google Analytics

The Service Offering utilizes Google Analytics to collect data directly from any browsers used to access and use the Service Offering. The data collected and inferred is used by VMware to diagnose and improve its products and services, and to address issues. Further information on how Google collects and uses this data when you use the Service Offering can be found at www.google.com/policies/privacy/partners/.

For users who wish to opt out of Google Analytics, Google makes the following browser add-on available: https://tools.google.com/dlpage/gaoptout.

You agree to provide the information, above, regarding Usage Data, FullStory, and Google Analytics usage to all Users of the Service Offering.

Microsoft Server Products

If you are running Windows workloads in your Service Offering instance and wish to leverage the functionality of the Microsoft Windows Server Datacenter offering or the Microsoft SQL Server Enterprise offering (collectively, the "Microsoft Products"), you may have VMware enable the Microsoft Products, under VMware's own licenses for the Microsoft Products, for your environment. VMware is a licensee of the Microsoft Products pursuant to a separate agreement between Microsoft and VMware. You may be able to provision your existing license(s) in your environment, if those licenses are eligible for that portability, pursuant to your own license agreement with Microsoft.

If you elect to have VMware enable the Microsoft Products for your Service Offering instance, VMware will charge you for this use. Consult your VMware sales specialist for details.

Your use of the Microsoft Products is subject to the following conditions, which are in addition to the provisions of the Agreement:

1. **The Microsoft Products may only be used with your instance of the Service Offering. You are not permitted to provision or to allow anyone else to provision the Microsoft Products in any other environment, including but not limited to your on-premises environment.**
2. The Microsoft Products may not be used in high-risk activities, as described in the TOS.
3. You may not remove, modify or obscure any copyright, trademark or other proprietary rights notices that are contained in or on the Microsoft Products;
4. You may not reverse engineer, decompile, or disassemble the Microsoft Products, except to the extent that such activity is expressly permitted by applicable law;
5. Microsoft, to the extent permitted by applicable law, disclaims all warranties regarding, and any liability on the part of Microsoft or its suppliers for any damages, whether direct, indirect, or consequential, arising from, your use of the Service Offering;
6. The Microsoft Products are the intellectual property of Microsoft. Your rights to use the Microsoft Products are limited to those rights expressly granted in the Agreement and are subject to the conditions in this section.
7. Microsoft is a third party beneficiary of this agreement, with the right to enforce these terms and to verify your compliance with these terms.

If you need support for the Microsoft Products, you must contact Microsoft, or your preferred third-party support provider. VMware will not provide support for the Microsoft Products you use in connection with your Service Offering instance.

NOTE: The separate license agreement between VMware and Microsoft regarding the Microsoft Products requires VMware and/or your authorized VMware channel partner to disclose your name and address to Microsoft, and you acknowledge this and consent to this disclosure (i) if you have a demonstration of the Service Offering, using the Microsoft Products, or (ii) if you use the Service Offering on a trial or evaluation basis and the Microsoft Products are used. If you elect to have VMware provision the Microsoft Products in your Service Offering instance, VMware is also required to disclose to Microsoft the country in which your instance of the Service Offering is provisioned, and you acknowledge and consent to this disclosure. This information will be used by Microsoft to verify VMware's compliance with the terms of the separate license agreement between VMware and Microsoft regarding the Microsoft Products, and your compliance with the terms set forth above in this section.

Service Operations

Support

To obtain live support for the Service Offering, please use the Chat function by clicking on the "Support" tab, or as an alternative, create a Support Request at: https://console.cloud.vmware.com/csp/gateway/portal/#/support.

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

VMware support includes all aspects of the SDDC components, and the underlying AWS bare metal instance types. This includes support for virtual machines, containers, and supported guest operating systems. In addition, VMware will provide commercially reasonable assistance with installation, configuration, and troubleshooting of supported applications, including but not limited to Microsoft, Oracle, and VMware Technology Partners. See: https://www.vmware.com/resources/compatibility/search.php?deviceCategory=vsanps&details=1&releases=302&page=1&display_interval=10&sortColumn=Partner&sortOrder=Asc

In order to receive support, you must be on a supported version of the Service Offering. For supported versions, see: https://docs.vmware.com/en/VMware-Cloud-on-AWS/services/com.vmware.vmc-aws-operations/GUID-90811917-AC7A-48CF-9176-435529E0F6E2.html

If you are not on a supported version of the Service Offering: (i) VMware reserves the right to decline support until you are on a supported version, and (ii) VMware cannot guarantee the availability metric set forth in the Service Level Agreement nor that you will be entitled to any service credits otherwise available pursuant to the Service Level Agreement.

Service Provisioning

Customers can provision and resize their SDDCs on demand, using the VMC Console. An SDDC includes a minimum of one cluster with a single host. Customers can add hosts and clusters, up to the provisioning maximum for their organization. Customers can select the available AWS region where their SDDCs will be provisioned.

VMware will delete "failed" hosts in your SDDC. For purposes of this Service Description, a "failed host" is (i) a host that was never successfully deployed, so it has never been consumed by the customer, or (ii) a host that the customer attempted to delete but the deletion action has failed. In

either case, when these hosts show as inactive for seven days, they will be deleted. They will also show as "failed" in the Service Offering console.

Capacity Management

Customers are responsible for capacity management of their SDDCs. VMware requires that 30% unused space ("slack space") be maintained in the VMware vSAN™ datastore within the Service Offering, to support operation of the SDDC. Adequate slack space is required for use of the vSAN datastore. If storage free space reaches (or falls below) 25%, it is possible that the customer could lose the ability to utilize the SDDC, and the environment could become inoperable. If unused space in an SDDC vSAN datastore drops reaches (or falls below) 25%, VMware will automatically add hosts to the SDDC to prevent damage to the SDDC. Customers can use the VMware Cloud sizer tool, found at https://vmcsizer.vmware.com/home, for guidance on the appropriate number of hosts needed to support anticipated workloads.

If you have changed the Elastic DRS for VMware Cloud™ on AWS (Elastic Distributed Resources Scheduler) ("eDRS") policy to "Optimize for Best Performance" or "Optimize for Lowest Cost", we will automatically size your SDDC up or down based on load and according to the eDRS policy you have chosen. If you do not change your eDRS settings, the default option is "Scale Up for Storage Only" which means that we will add hosts to your SDDC only when storage capacity becomes critical (that is, 25% or less free space). When eDRS is set to "Scale Up for Storage Only" we will not automatically scale your SDDC down.

Unless you and we otherwise agree, additional hosts added pursuant to this capacity management process will be billed at the then-current published on-demand rate for as long as those hosts are provisioned.

Amazon Web Services Account

You will not be able to access or use the Service Offering without having your own AWS customer account (an "AWS account"), which you must establish directly with AWS. This means that if you do not already have an AWS account, you must establish one prior to being able to access the Service Offering. See https://aws.amazon.com/agreement/ for the current form of the AWS Customer Agreement. If you have questions on the AWS Customer Agreement, you must contact AWS.

Prior to provisioning an SDDC, we require customers to connect to their AWS account. This process establishes identity and access management policies in your AWS account that enable communication between resources provisioned in your AWS account and in the SDDC.

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 availability of the Service Offering.

You are responsible for incident and problem management (e.g., detection, severity classification, recording, escalation, and return to service) pertaining to all virtual machines that you have deployed in your SDDC.

Data Recovery

We will provide the following backup and restore services:

- Management infrastructure, including VMware vCenter Server®, VMware NSX® Manager™, VMware NSX® Controller™, and VMware NSX® Edge™

You are responsible for backup and restoration of the following:

- All Content and configurations created by you in the SDDC, including virtual machines, content libraries, datastores, and port groups.

Change Management

We will provide the following change management services:

- Processes and procedures to maintain the health and availability of the Service Offering.
- Processes and procedures to release new code versions, hot fixes, and service packs related to the Service Offering.

Updates to the SDDC software are necessary to maintain the health and availability of the overall Service Offering, and are mandatory. These updates will be applied to your SDDC, subject to the processes set forth in this section. A customer may not, in the normal course, skip or delay application of these updates. If a customer is not on the current version of the SDDC software, we will not guarantee support for the affected SDDCs.

We will provide notification of scheduled maintenance at least 24 hours in advance for any changes that may impact your use of an SDDC. Changes related to maintenance may require maintenance downtime for SDDC management servers of up to 40 hours per year for each SDDC.

Service Location

The Service Offering is deployed in AWS data centers in multiple regions. You select the AWS region where your SDDC will be deployed, and your workloads will persist in that data center. VMware will not change the AWS region in which your SDDC is deployed without your prior authorization. The VMC Console data, including your SDDC configuration information and data that VMware collects relating to your use of the Service Offering, persists in the AWS US-West (Oregon) data center location, but may be replicated to other AWS regions to ensure availability of the Service Offering.

Security

The end-to-end security of the Service Offering is shared between VMware and you. The primary areas of responsibility between VMware and you are outlined below.

We will use commercially reasonable efforts to implement reasonable and appropriate measures designed to help you secure Your Content against accidental or unlawful loss, access, or disclosure, including the following:

- **Information Security**: We will protect the information systems used to deliver the Service Offering over which we (as between VMware and you) have sole administrative level control.

- **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 Offering over which we (as between VMware and you) have sole

administrative level control. This responsibility stops at any point where you have some control, permission, or access to modify an aspect of the Service Offering.

- **Patching and Vulnerability Management**: We will maintain the systems we use to deliver the Service Offering, 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 Offering. Critical vulnerabilities will be addressed in a timely manner.

You are responsible for addressing the following:

- **Information Security**: You are responsible for ensuring adequate protection of the Content that you deploy and/or access with the Service Offering. This includes, but is not limited to, any level of virtual machine 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 in all SDDCs that you deploy in the Service Offering.

- **Security Monitoring**: You are responsible for the detection, classification, and remediation of all security events that are isolated with your deployed SDDCs, associated with virtual machines, 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.

You must not upload, host, store, or process any Content that is restricted as specified in Section 3.2 of the Terms of Service.

Security Updates and Maintenance

VMware requires customers to be on supported versions of the Service Offering to maintain the functional integrity and security of the Service Offering. See the “Support” section, above, for guidance on determining supported versions. All customers must comply with scheduled maintenance, as notified by VMware, and all required upgrades to move to a supported version of the Service Offering. Some updates to the Service Offering may be required for security, performance, availability, or stability reasons, including for issues that may affect all customers of the Service Offering. In most cases, a customer will be given a minimum of seven days’ notice for scheduled maintenance. VMware will use commercially reasonable efforts to provide 24 hours advance notice prior to any emergency maintenance. However, critical security vulnerabilities updates may be implemented by VMware with no advance notice. Customers may not refuse, reschedule, or postpone emergency maintenance. VMware will take commercially reasonable steps to minimize emergency maintenance.

Data Encryption

The Service Offering applies multiple layers of encryption for data stored in the SDDC.

At the physical layer, data on NVMe drives residing in the hosts making up the SDDC is encrypted using an XTS-AES-256 cipher implemented on a hardware module on the host. The encryption keys are generated using the hardware module and are unique to each NVMe drive. All encryption

keys are destroyed when the host is terminated and cannot be recovered. You cannot disable this encryption and you cannot provide your own encryption key

At the vSAN layer, all SDDC data resides in vSAN Data Stores and is encrypted using FIPS 140-2 compliant encryption. All encryption keys are stored in AWS Key Management Server (KMS) and are managed by VMware. Customers have the option to rotate their vSAN encryption key (KEK) by following the instructions provided in the documentation.

At the Virtual Machine layer, customers have the option to use in-guest encryption solutions and retain full control over their encryption keys. A variety of software solutions are available that can be used for this including Microsoft BitLocker, Thales CipherTrust, and others found in the VMware Marketplace at:
https://marketplace.cloud.vmware.com/services/?deployment-platforms=vmc.

Time Synchronization

The Service Offering utilizes time synchronization across all SDDC components to ensure clock consistency in events and logs. All SDDC components are configured to use the Coordinated Universal Time (UTC) standard synchronized by the AWS Time Sync service using the NTP protocol. Customers are encouraged to synchronize time in their virtual machines against the AWS Time Sync service for end-to-end consistency.

PCI Compliance

VMware Cloud on AWS is certified as a PCI DSS Level 1 Service Provider, the highest level of assessment available. The compliance assessment was conducted by Coalfire Systems Inc., an independent Qualified Security Assessor (QSA). After initial deployment of an SDDC, the customer may choose to configure it for PCI compliance. Once configured for PCI, the customer must affirmatively take steps to disable several SDDC add-on capabilities in order to maintain compliance, including VMware HCX. VMware will provide a customer-facing website, listing compliant offerings, that customers can reference to ensure that they disable non-compliant VMC add-ons to maintain PCI compliance for their VMC on AWS environment. In addition, once an SDDC is configured for PCI compliance, the Networking and Security configuration will be managed directly via the NSX Manager deployed in the SDDC rather than by the VMC Console. For more details, refer to the documentation at docs.vmware.com. See the following for VMware Cloud on AWS Regions that are available for deployment of PCI compliant SDDCs: AWS Region and Availability Zone Support.

Before deploying any other or add-on VMware service in your instance of the Service Offering, you should review the interoperability and compliance information for that service. See https://cloud.vmware.com/trust-center/compliance the most current information on compliant offerings. You are responsible for ensuring that any additional service deployed in your Service Offering instance meets your compliance and security requirements.

VMware HCX® (Included)

VMware HCX delivers secure and seamless app mobility and infrastructure hybridity across vSphere 5.0+ versions, both on-premises and in the cloud. If you elect to configure VMware HCX, the Service Offering will automatically provision necessary components to enable VMware HCX in your SDDC.

For additional information on VMware HCX, see https://cloud.vmware.com/vmware-hcx

VMware Site Recovery™ for VMware Cloud™ on AWS (Optional)

VMware Site Recovery™ for VMware Cloud™ on AWS expands and simplifies traditional disaster recovery operations by delivering on-demand site protection across a common, vSphere-based operating environment from on-premises to the cloud. VMware Site Recovery protects workloads between on-premises datacenters and VMware Cloud, as well as between different instances of VMware Cloud. VMware Site Recovery is available for an additional fee.

If you elect to use VMware Site Recovery, we will automatically provision the necessary components in your instance of the Service Offering to enable VMware Site Recovery.

You are responsible for the following:

- Configuring network connectivity between your environment and the SDDC
- Configuring VMware Site Recovery in your on-premises environment to protect workloads

For additional information on VMware Site Recovery, see https://cloud.vmware.com/vmware-site-recovery.

Business Operations

Billing and Usage Metering

Purchasing the Service Offering

The Service Offering is offered on an on-demand basis, or customers can purchase committed term subscriptions for either a one-year or a three-year term. A customer can elect to pay base (committed) charges (which are the charges for reserved host capacity) for the subscription term either up front (that is, all in advance) or in monthly payments. If a customer elects to pay in monthly installments, the customer is still obligated to pay all base (committed) charges for the full one-year or a three-year term. Customers are also obligated to pay any additional charges that may be incurred through use of the Service Offering, as described below.

You can pay charges for the Service Offering (i) by credit card, (ii) through redemption of VMware's Subscription Purchasing Program (SPP) credits or Hybrid Purchasing Program (HPP) credits (collectively, "Credits"), or (iii) by using a purchase order (PO) and invoice process.

If you elect to pay for the Service Offering through redemption of Credits, then as you use the Service Offering, your Credit fund will be decremented, or charged, for your use of the services. If you use Credits as a payment method and your Credit fund is depleted, the Credit fund may go into an "overage" state and you will need to purchase additional Credits to true up the fund's negative balance.

Refer to the following websites for information on the Credit programs:

- SPP Program Guide: https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/solutions/vmware-spp-program-guide.pdf
- HPP Program Guide: https://www.vmware.com/files/pdf/solutions/vmware-hpp-program-guide.pdf.

If you elect to pay for the Service Offering by using a credit card as a form of payment, you will be charged a nonrefundable fee of $2,000 USD or equivalent in your applicable non-USD currency, upon deployment of your first SDDC. If, for any reason, the charge is rejected by our credit card processor, we will suspend your account, and you will not be able to access or use

the Service Offering. If the charge is accepted, then you will have 60 days within which to accrue fees against the amount charged. Any unused portion of the initial charge remaining at the end of the 60-day period will not be refunded and may not be used to pay for any cloud service offerings. You will be invoiced for any fees accrued in excess of the initial $2,000 USD charge.

One-Node Offering

For customers wishing to use the Service Offering for certain use cases, VMware offers a limited-scope offering, consisting of an SDDC comprised of one node. Not all features and functionality of the standard Service Offering are available in this limited scope offering. The VMware Cloud on AWS Service Level Agreement does not apply to this one-node offering. This one-node offering is not eligible for any updates or upgrades that are applied to the standard Service Offering. You can upgrade to a standard SDDC configuration from this one-node offering at any time during the permitted use period.

You will be billed for use of this one-node offering at VMware's standard on-demand rates unless you purchase a committed term subscription for the offering. Your permitted use period for the one-node offering is limited to 60 days (although you are not required to use the one-node offering for the full 60-day period). Any Content remaining in this one-node SDDC at the end of that 60-day period will be deleted. You may be able to purchase additional 60-day use entitlements, subject to availability. Payment for the one-node offering is available via credit card, redemption of SPP/HPP credits, or a PO and invoice. For availability and details on pricing, consult your VMware sales representative.

Billing

If you consume the Service Offering on an on-demand basis, you will be billed monthly, in arrears, for both host capacity and metered use charges. "Metered usage charges" are IP address usage, IP address remaps, egress data, and protected VMs.

If you purchase a committed term subscription for the Service Offering, and elect to pay base charges in full, in advance, you will be billed up front for reserved host capacity for the term of the subscription. If you purchase a committed term subscription with monthly payments, you will be billed on a monthly cycle for the duration of the one-year or three-year term commitment.

For a committed term subscription, regardless of whether you choose to pay committed base charges in full up front, or on a monthly basis, you will also be billed in arrears, at on-demand rates, for (i) metered usage charges and (ii) any reserved host usage in excess of the committed capacity purchased in your subscription. You will also be billed for any additional capacity provisioned by VMware to maintain the health of your SDDC environment (as described in "Capacity Management", above).

For additional information on pricing, see https://cloud.vmware.com/vmc-aws/pricing.

You will also receive a separate bill from AWS for services that you receive directly from AWS, through your AWS account.

Expiration of Committed Subscription Term

Committed term subscriptions do not renew at the end of the purchased subscription term. If you wish to purchase additional committed term subscriptions, those Subscription Terms will not be coterminous with any subscriptions previously purchased.

Unless you purchase a new subscription, upon expiration of a committed subscription term, if you continue to use the Service Offering after expiration of your committed subscription term, all

services will continue to operate on an on-demand basis, and you will be billed at the then current on-demand rate for those services until you cancel your on-demand use.

Cancellation

You may cancel your use of the Service Offering as described below:

- If you are using the Service Offering on an on-demand basis, you can cancel at any time by deleting your SDDC, using the VMC Console. You will be charged for all usage up to the point of termination.
- If you purchase an entitlement to the Service Offering via a one-year or a three-year subscription (regardless of whether you have elected up front or monthly payments), you cannot cancel or terminate your subscription prior to the expiration of the purchased Subscription Term. You are liable for all charges accruing during the Subscription Term, regardless of whether you actually use the Service Offering for the entire Subscription Term. You may delete your SDDC, using the VMC Console, to avoid incurring metered usage charges. There is no refund for any committed charges that you paid at the time you purchased your subscription.

Suspension and Re-Enablement

During the time your access to and use of the Service Offering is suspended for any reason as provided in the Terms of Service, we may restrict access to all your account's SDDCs, VMs, and service consoles.

Re-enablement of your account will be initiated promptly upon resolution of the issues that led to suspension, and access to the Service Offering(s) and your SDDCs will be restored. Failure to resolve the reason for suspension may result in termination of your account, as provided in the Terms of Service.

Termination

You are responsible for backing up and migrating all workloads to your target environment, and deleting your SDDCs, prior to termination of your Subscription Term (whether it terminates through expiration or as otherwise provided in the Terms of Service). You can utilize one of multiple backup appliance vendors certified by VMware to perform workload backup and migration. For further information, contact your VMware sales specialist.