vmware®

Service Description

VMware Cloud™ on AWS

Last updated: 13 January 2020

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

vmware®

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:
  - o VMware vSphere® running on elastic bare metal hosts deployed in AWS
  - o VMware vCenter Server® appliance
  - o VMware NSX® Data Center to power networking for the Service Offering
  - o VMware vSAN™ aggregating host-based storage into a shared datastore
  - o 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, or directly at: https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/downloads/eula/vmware-cloud-services-universal-tos.pdf.

Usage Data

The Service Offering collects data directly from the machines and/or devices involved in the use of the Service Offering, such as configuration, performance, and usage data, to improve VMware products and services, 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

Rev. 13 Jan 2020

any of this data is considered personal data under applicable data protection laws, the data will be treated in accordance with the VMware Privacy Notice, found at: https://www.vmware.com/help/privacy.html.

In connection with the collection of usage data, VMware and its service providers use cookies. Detailed descriptions of the types of cookies we use can be found in the VMware Privacy Notice and policies linked from the VMware Privacy Notice. More information on how to choose whether to accept certain cookies used by VMware websites and solutions can also be found from that link.

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.

Service Operations

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.

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.

Rev. 13 Jan 2020

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. 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 provide:

- **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.

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.

See https://cloud.vmware.com/vmc-aws/pricing for the latest information on pricing for the Service Offering.

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, at 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 30 days (although you are not required to use the one-node offering for the full 30-day period). Any Content remaining in this one-node SDDC at the end of that 30-day period will be deleted. You may be able to purchase additional 30-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.

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. Notwithstanding the foregoing, if you wish to extract your Content from the Service Offering (to the extent you have not already done so prior to termination of your Subscription Term), you must notify us within five (5) days after the effective termination date, and we will assist you in extracting Content from the Service Offering. You will be responsible for all fees associated with Content extraction. If you do not notify us within that 5-day period, your Content will be permanently deleted and will not be recoverable.