Service Description

VMware Cloud™ on AWS GovCloud (US)

Last Updated: 14 August 2020

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.

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

Introduction

The VMware Cloud™ on AWS GovCloud (US) cloud service offering (a "Service Offering" as defined in the Terms of Service) brings VMware's enterprise class software defined data center software to the Amazon Web Services GovCloud (US) region, 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
- Self-service provisioning of SDDCs
- Maintenance, patching, and upgrades of the SDDC, performed by VMware

Service Consoles

The Service Offering includes access to the following consoles:

- VMware GovCloud Service Console is the primary point of entry into the service and is accessed at console.cloud-us-gov.vmware.com
- VMware Cloud on AWS GovCloud Console (the "VMC Console") is the primary interface for provisioning SDDCs at www.vmc-us-gov.vmware.com
- VMware vSphere® client (in the customer SDDC) provides access to manage workloads and the compute, storage, and network components of the SDDC.
- VMware GovCloud status page (status.gov.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.

FedRAMP Authorization

The Service Offering is currently "In Process" for FedRAMP High authorization, but does not currently have a FedRAMP Authority to Operate ("ATO"). To comply with FedRAMP High requirements, customers must select EC2 i3en.metal host type when deploying an SDDC. When you are in the Service Offering's portal, you can choose either the EC2 i3.mel *OR* the EC2 i3en.metal. However, *only* the EC2 i3en.metal host type will be included in the FedRAMP

certification. If you choose the EC2 i3.metal host, that host will not be compliant with FedRAMP High certification. If you need FedRAMP, you must choose the correct type of host.

Check the FedRAMP Marketplace https://marketplace.fedramp.gov for the latest status of our authorization.

Availability of Add-on Services

Core functionality of the VMware Cloud on AWS GovCloud SDDC, such as compute, storage, and networking, is equivalent to the functionality available in the commercial VMware Cloud on AWS offering (i.e., VMware Cloud™ on AWS). However, some optional add-on services available in the commercial VMware Cloud on AWS offering are not available, and may never be available, in the VMware Cloud on AWS GovCloud (US) offering due to technical limitations and security requirements. Refer to the table below for key differences.

Add-on Service	VMware Cloud on AWS	VMware Cloud on AWS GovCloud (US)
VMware vRealize Log Insight Cloud	Available	Not Available
VMware HCX	Available	Not Available
VMware Site Recovery	Available	Not Available
VMware Cloud Marketplace	Available	Not Available
VMware vRealize Network Insight Cloud	Available	Not Available

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 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 uses 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.

You agree to provide the information, above, regarding Usage Data to all Users of the Service Offering.

Service Operations

Support

We will provide support for problems that you report to assist with onboarding to the Service Offering. For ongoing support, customers must purchase a separate US Federal Support offering (see https://www.vmware.com/support/services/usfed.html). To obtain support for the Service Offering, please call VMware Federal Support at 877-869-2730. Note that Chat support is not available in the Service Offering.

Amazon Web Services Account

You will not be able to access or use the Service Offering without having your own AWS GovCloud (US) customer account, which you must establish directly with AWS. This means that if you do not already have an AWS GovCloud (US) account, you must establish one prior to being able to access the Service Offering. See the "Getting Started & Logistics" section of https://aws.amazon.com/govcloud-us/faqs/ for details. 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.

User Provisioning and Management

Unlike the VMware Cloud on AWS commercial offering (VMware Cloud™ on AWS), this Service Offering requires customers to provide their own infrastructure to manage user provisioning and access. As part of provisioning the Service Offering, the VMware Customer Success team will work with the customer to configure user authentication against a customer-maintained Active Directory Federation Service (ADFS) server. Customers typically utilize an existing on-premise Microsoft ADFS server, or alternatively a service like AWS Directory Service (https://aws.amazon.com/directoryservice/) or Azure Active Directory Domain Services (https://azure.microsoft.com/en-us/services/active-directory-ds/) for this purpose.

SDDC Provisioning

Customers can provision and resize their SDDCs on demand, using the VMC Console. A production SDDC includes a minimum of one cluster with three hosts. Customers can add hosts and clusters, up to the provisioning maximum for their organization. Configuration maximums for the Service Offering can be found at https://docs.vmware.com/en/VMware-Cloud-on-AWS/services/com.vmware.vmc-aws-operations/GUID-10A0804B-04F4-4B8A-9EBA-85169F533223.html

Capacity Management

Customers are responsible for capacity management of their SDDCs. VMware requires that 30% unused space ("slack space") be maintained in the 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.

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 the AWS GovCloud (US-WEST) region. 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 GovCloud (US-WEST) data center location.

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.

Business Operations

NOTE: United States federal government customers are subject to specific rules on purchasing entitlements to the Service Offering. If you are a US federal government customer, consult your VMware sales representative for details on purchasing an entitlement to the Service Offering, including billing arrangements.

Billing and Usage Metering

Purchasing the Service Offering

See https://cloud.vmware.com/govcloud/pricing for the latest information on pricing for 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. Customers are also obligated to pay any additional charges that may be incurred through use of the Service Offering, as described below.

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. Note that due to legal rules, US federal government customers may be not be able to purchase one-year and three-year subscriptions and limited only to purchasing on-demand.

For a committed term subscription, 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).

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, 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.