NOTICE: This Service Description is no longer being updated. Content has been moved to the Cloud Services Guide at:

https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/agreements/vmware-cloud-services-guide.pdf

Service Description

VMware Cloud™ on AWS Outposts

Updated:07 September 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, or VMware International Unlimited Company, a company organized and existing under the laws of Ireland, if the billing address for your order is outside the United States. Terms not defined in this Service Description are defined in the Terms of Service or elsewhere in the Agreement.

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 Outposts (the "Service Offering") delivers the VMware Software Defined Data Center to a customer's location, in a fully managed service with AWS Outposts.

The Service Offering has the following components:

- The VMware Software Defined Data Center ("SDDC"), consisting of:
  - VMware vSphere®
  - 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
- Maintenance, patching, and upgrades of the AWS Outposts performed by AWS

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

Service Operations Data

In connection with providing the Service Offering, VMware collects and processes information (such as configuration, performance, and log data) from the SDDC and the AWS Outposts, and from the customer's systems, applications, and devices that are used with the Service Offering. 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 (such as configuration, performance, and usage data) directly from the SDDC and the AWS Outposts, and from the customer's systems, applications, and devices involved in the use of the Service Offering, to improve VMware products and services, and your and your users' experiences, as more specifically described in VMware's Trust & 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 VMware's Privacy Notice, including the VMware Products and Services Notice available 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 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.

Service Offering Provisioning

Customers can provision and resize their SDDCs on demand, using the VMC Console. An instance of the Service Offering includes includes a minimum of one physical rack with three hosts. Customers can add hosts and clusters, up to the provisioning maximum. Customers can select the available AWS region where their SDDCs will be connected.

Subscriptions to the Service Offering are offered for committed terms of three years. If your business requires a shorter subscription term, please consult your VMware sales representative. Your Subscription Term begins on the earlier of (i) the date on which you deploy the first SDDC on the system, or (ii) 10 days after you have been notified that the system is ready for SDDC deployment.

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 if there is available dark capacity in the rack.

Elastic DRS (Elastic Distributed Resources Scheduler, or eDRS) is configured as "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, as well as the physical environment and dependencies in your location for VMware Cloud on AWS Outpost racks.

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 in connection with support, we will handle that content in any such country in accordance with the Terms of Service. VMware is the single point of contact for all Service Offering support requests. Hardware break/fix support will be performed by AWS or AWS's approved third-party partners. Full availability of the Service Offering is dependent upon and subject to the performance of the AWS hardware and infrastructure components.

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 of Your 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 Offering Location

The Service Offering is deployed at the customer premises location(s) ("Designated Facility") specified by the customer when ordering. The fully assembled and pre-configured rack ("the system") will be shipped to that/those location(s).

An AWS technician must be provided access to the installation location(s) in a timely manner for the following activities:

- Initial site survey of the Designated Facility – this is an onsite visit by an AWS technician to validate that the Designated Facility condition and networking meet requirements for installation of the system.
- Installation of the system at the Designated Facility.
- Remediation of a problem with the Service Offering (e.g., needing to replace faulty AWS Outposts) when the issue cannot be addressed remotely.
- Retrieval of the system from the Designated Facility.

You will not require AWS personnel to sign, accept, or otherwise agree to any documentation as a condition of accessing the Designated Facility, and you agree that the terms of any such documentation are void even if signed by AWS personnel. You will ensure that no one accesses, moves, or repairs the AWS Outposts other than (i) personnel designated by AWS, (ii) as permitted in writing by AWS in connection with the maintenance of the AWS Outposts, or (iii) as necessary due to a situation involving imminent injury, damage to property, or an active fire alarm system. You will ensure that no one modifies, alters, reverse engineers, or tampers with the AWS Outposts. You acknowledge that the AWS Outposts may be equipped with tamper monitoring features.

The Service Offering is linked to AWS regions. You select the AWS region where your SDDC will be managed. VMware will not change the AWS region in which your SDDC is managed 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 cloud.

You will ensure that at all times the Designated Facility meets the minimum requirements necessary to support the installation, maintenance, use, and removal of the system, as defined here. VMware is not responsible for any delay in installation or any failure of the AWS Outposts

or the SDDC if the customer does not maintain the specified environmental conditions at the Designated Facility.

You are not permitted to move the system from one location (premises) to another (e.g.,in connection with a site consolidation), or to relocate the system within the Designated Facility premises. Any move or relocation of the system must be completed by an AWS technician. You must contact VMware in advance of any planned move or relocation. A fee may be charged for services to move or relocate the system.

You must ensure that you have all necessary rights, certifications, and licenses for the delivery, installation, maintenance, use, and removal of the system at the Designated Facility. You are responsible for any damage to the system while it is at the Designated Facility, unless caused by AWS.

Restriction on Modification of System

The rack is a closed system, for use solely with the Service Offering. Customers are not allowed to physically interact with or modify the system in any way, nor to modify the Service Offering software except as expressly permitted. All interactions with the Service Offering must be through the VMware Cloud Console, except the vCenter Service Appliance, which can be accessed through the Service Offering console, or from within the customer's SDDC through the uplink connection.

When you receive the system at the Designated Facility, you must not open or disturb the package containing the system, and keep the package in a safe location at the Designated Facility until a AWS technician arrives to unbox the system, set it up, configure it, and power it on. Thereafter, any problems with the system will be handled through the support process.

If you directly access (except through direct vCenter access) or modify the system any way, it may result in relieving VMware of our support obligations, and VMware may choose to discontinue the Service Offering at the compromised location, and/or terminate your subscription

Service Offering Hardware

Title to the AWS Outposts remains at all times in AWS, and the customer acquires no right or interest in the AWS Outposts by virtue of ordering a subscription to the Service Offering. VMware reserves the right to replace the AWS Outposts (with the assistance of AWS) at a customer's location(s) at any time for any reason.

At VMware's discretion, AWS Outposts may be refreshed by AWS at the end of a customer's committed subscription term, depending on the length of the original subscription term and any renewal term. AWS Outposts will not be refreshed during a committed subscription term. In the event of an AWS Outposts refresh, VMware will assist the customer in migrating data and workloads to the new AWS Outposts.

Service Offering Communications

The Service Offering requires sustained network connectivity to the AWS cloud via the AWS Outposts service link. The performance and stability of this connectivity is the customer's responsibility. Excessive latency or interruption of this connectivity could result in a disruption of support capabilities or availability of the Service Offering. VMware may be relieved of support obligations in instances where network connectivity is unstable or exhibits regular excessive latency.

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 Your Content and any other content that you 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.
- **Physical security of the system**: You are responsible for ensuring the physical security of the system at each Designated Facility.
- **Insurance against damage, theft and vandalism of the system**: You are responsible for purchasing insurance to adequately protect against physical risks such as earthquakes, or accidents inside the Designated Facility that could damage or destroy the system installed at each Designated Facility. At a minimum this must cover the replacement of the AWS Outposts. You may, at your option, also purchase insurance to compensate you in the event of business interruption, loss of data, and other risks, including cyber-security incidents.

- **Upon subscription termination, removal of all sensitive data**: After the end of your subscription term, an AWS technician will retrieve the system from your Designated Facility. You are responsible for ensuring that Your Content has been removed from the system within the time period specified below.

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

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.

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

Business Operations

Purchasing Subscriptions to the Service Offering

You can purchase an entitlement to the Service Offering as a committed term subscription for three years. Base (committed) charges for the three-year subscription term are payable up front (that is, all in advance). Customers are also obligated to pay any additional charges that may be incurred through use of the Service Offering, as described below.

If you wish to purchase additional subscriptions to the Service Offering during a then-current Subscription Term, the terms of those additional subscriptions will not be coterminous with any subscriptions previously purchased.

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 through redemption of VMware's Subscription Purchasing Program (SPP) credits ("Credits"). If you do pay via 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 SPP Credit program:

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

Billing

In addition to the charges for your committed host capacity, you will also be billed in arrears, at on-demand rates, for (i) metered usage charges (for usage in excess of committed capacity), and (ii) any other in-region services (e.g., AWS EIP (Elastic IP address functionality), VTGW (Virtual Transit Gateway), etc.). You will also be billed for any additional capacity provisioned by VMware to maintain the healof 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. Unless you purchase a new subscription, 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 cease your on-demand use or until your ability to use or access the Service Offering is terminated.

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 provisions of this section, 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 committed subscription term), you will have forty-five (45) days after termination of your committed subscription term within which to notify us that you wish to extract Your Content and to complete that extraction, before an AWS technician removes the system from your Designated Facility. If you request, we will assist you in extracting Your Content from the Service Offering. You will be responsible for all fees associated with Content extraction. If you do not notify us before the system is removed from your Designated Facility, Your Content will be permanently deleted and will not be recoverable.