NOTICE: This Service Description is no longer being updated.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 Dell

Updated as of: 22 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, 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 Dell (the “Service Offering”) is a VMware-managed cloud service offering that brings VMware’s enterprise class software defined data center (“SDDC”) software on Dell hardware to a customer’s on-premises environment.

The Service Offering has the following features:

- VMware SDDC, consisting of:
  - VMware vSphere ESXi™ running on Dell VxRail
  - VMware vCenter® Server Appliance™
  - VMware NSX® Data Center for vSphere® to power networking for the service
  - VMware vSAN™ aggregating host-based storage into a shared datastore
  - VMware HCX® enabling application mobility and infrastructure hybridity
  - VMware Tanzu services for modern application development
- Dell-supplied hardware – Dell VxRail, Dell servers and switches, racks, UPS, etc.
- VMware SD-WAN™ hardware appliance, and for remote management
- Customer self-service provisioning of SDDCs through https://vmc.vmware.com/
- Maintenance, patching, and upgrades of the SDDC, performed by VMware
- Maintenance, patching, and upgrades of the Dell hardware performed by VMware (Dell provides firmware, drivers, and BIOS updates)

In addition to above features, every rack also includes standby capacity; i.e., a spare host not configured as part of the running cluster. In the event of a hardware-related degradation, the spare host can be activated in order to replace an unhealthy host in the cluster. The impaired host can then be repaired remotely or swapped without affecting application uptime

Service Consoles

The Service Offering includes access to the following service consoles:

- VMware Cloud Services Console (console.cloud.vmware.com) provides a common entry point for many VMware cloud service offerings, including the Service Offering.
- VMware Cloud on Dell console accessible from the above common entry point is the primary user interface for provisioning and managing SDDCs.
- VMware vSphere® Client™ 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

A Getting Started guide, data sheet, release notes, and FAQ documents are available at https://docs.vmware.com/

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 (such as configuration, performance, and log data) 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. 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 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, to improve VMware products and services, 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 Notice and policies linked from that 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. 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 before a Dell-authorized technician removes the Service Offering hardware from your premises, and we will assist you in extracting Your Content from the Service Offering. You will be responsible for all fees associated with extracting Your Content. If you do not notify us before Service Offering hardware removal, Your Content will be permanently deleted and will not be recoverable.

Service Operations

Service Provisioning

You can order your SDDCs using the VMware Cloud Console. An SDDC includes a minimum of one rack with three hosts. You can add hosts to the rack, up to the maximum supported by the rack.

The Service Offering is offered for committed term subscriptions of either one year or three years. Your initial subscription term begins upon the earlier of (i) the time of activation/first use of the Service Offering, or (ii) 30 days after the system is ready to ship from the Dell facility ("ready to ship" means that the system is built, configured to customer specifications, and no further actions need to be taken prior to shipment to the customer's installation site).

Service Location

The Service Offering is deployed at the street address location(s) that you specified when ordering the Service Offering through the VMware Cloud Console. The fully assembled and pre-configured rack ("the system") will be shipped to that/those location(s).

NOTE: The Service Offering may not be available for deployment in all geographies. You must consult your VMware sales representative or your preferred VMware reseller for confirmation of the Service Offering's availability at your selected ship-to location.

You must allow a Dell-authorized technician access to the installation location(s) in a timely manner for the following activities:

- Initial site survey – In most cases, initial site survey information is collected through the VMware Cloud Console during the ordering process. In some cases, the customer may get a phone call to verify certain information. For complex deployments, an engineer may need to visit the installation site for an on-site survey.
- Installation of the system and activation of Service Offering.
- Remediation of a problem with the Service Offering (e.g., needing to replace faulty hardware) where the issue cannot be addressed remotely.
- Retrieval of the system from your installation site(s).

Any delays in providing access to the installation site(s) will affect the response times(s) we provide for any required on-site activities.

Each installation site must comply with the published environmental specifications for the Service Offering (e.g., temperature, humidity, power, etc.). VMware is not responsible for any delay in installation or any failure of the hardware or the SDDC if the customer does not maintain the specified environmental conditions at the installation site(s).

See https://docs.vmware.com/en/VMware-Cloud-on-Dell-EMC/index.html for the environmental specifications.

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 rack within your premises. Any move or relocation of the system must be done by a Dell or a Dell-authorized 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.

The VMware Cloud Console data, including your SDDC configuration information and data that VMware collects relating to your use of the Service Offering, persists in VMware owned, managed and controlled data repositories in the the AWS cloud.

VMware HCX®

VMware HCX, which is included as part of the Service Offering, delivers secure and seamless application mobility and infrastructure hybridity across vSphere, 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.

Application Modernization with VMware Cloud™ with Tanzu services (Included)

Tanzu services enable customers to run and manage the growing number of modern applications they have more effectively, and enable operators to deliver Kubernetes as a service through the VMware Cloud Console quickly and easily to developer teams.This fully managed Tanzu service is included in your subscription to the Service Offering.

VMware Site Recovery™ (Optional Add-On)

VMware Site Recovery™ for VMware Cloud™ on Dell 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 is available for an additional fee. If you elect to use VMware Site Recovery, we will provision the necessary components in your instance of the Service Offering.

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

Capacity Management

You are responsible for storage capacity management of your SDDCs. VMware requires that 25% unused space (“slack space”) be maintained in the vSAN datastore within the Service Offering, in order to support operation of the SDDC. Adequate slack space is required for use of the vSAN datastore. If storage free space falls below 25%, it is possible that you could lose the ability to utilize the SDDC, and the environment could become inoperable.

Support

VMware is the single point of contact for all Service Offering support requests. Hardware break-fix support will be performed by Dell or Dell’s approved third-party partners for specific infrastructure elements like UPS, PDU, etc., upon request from VMware.

Full availability of the Service Offering is dependent upon and subject to the performance of the Dell hardware components, and of the AWS infrastructure on which the VMware Cloud Console is hosted.

The Service Offering provides customers with management access to the SDDC through vCenter. This availability is subject to (i) availability and performance of the Service Offering hardware, (ii) loss of power or internet connectivity at the customer installation site, (iii) availability of the AWS infrastructure, (iv) scheduled maintenance where you have been notified at least 24 hours in advance, (v) recurring or zero-impact maintenance that is generally applicable to all customers, (vi) customer’s misuse of the Service Offering or any Service Offering component, (vii) force majeure events, denial of service attacks, viruses, or hacking attacks for which there is no commercially reasonable known solution, or any other events that are not within our control or that could not have been avoided with commercially reasonable care, (viii) acts or orders of government, (ix) packet loss, network or internet problems beyond VMware's border router supporting our public internet connectivity, or (x) bugs in code or services for which there is no commercially reasonable known fix (even if there is a known workaround).

Incident Response

VMware is committed to rapid response on all support requests. Incident Response times for all severities are the same as the response times specified in the current VMware Support Policies

The VMware production support offering applies to your use of the Service Offering. See https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/support/vmware-saas-production-support-and-subscription-datasheet.pdf.

Incidents of all severities can be logged with VMware on a 24 hours per day, 7 days per week, 365 days per year basis via phone, web, or chat (restricted hours for live chat). Severity Level response times do not vary whether the support request is filed via phone, web, or chat. VMware does not guarantee resolution times, and a resolution may consist of a fix, workaround, service availability, or other solution VMware deems reasonable.

Hardware Break-fix

Following completion of remote troubleshooting, diagnosis, and problem determination, VMware and Dell will determine if the qualified incident requires an on-site technician and/or parts to be dispatched, or if the issue can be resolved remotely. If an onsite service call is required, then the response times will be as set forth below.

Type of Onsite Response	Onsite Response Time	Restrictions / Special Terms
Four-hour mission critical onsite response for hosts. Note: The rest of the rack infrastructure (e.g., switch,UPS, PDU, etc.) is Next Business Day	A Dell-authorized technician typically arrives onsite within four hours **after** completion of diagnosis and troubleshooting by VMware and Dell, VMware and Dell have isolated the problem, and have deemed an onsite response necessary.	• Available within defined four-hour response locations. If the location is outside of the supported region, support will default to Next Business Day. In either cases, a technician will need access to the hardware for the fix. • Available seven days each week, 24 hours each day, including holidays • Four-hour response time is provided only for break-fix on hosts. All other hardware components within the VMC on Dell infrastructure (switches, PDUs, and UPS) will be replaced within the Next Business Day
Next Business Day onsite response	A Dell-authorized technician typically arrives onsite Next Business Day **after** completion of	• Next Business Day response time is provided for break-fix on switches, PDUs, and UPS

Type of Onsite Response	Onsite Response Time	Restrictions / Special Terms
	diagnosis and troubleshooting by VMware and Dell, they have isolated the problem, and deemed onsite response necessary.	within the VMC on Dell infrastructure • Available five days each week, 10 hours each day, excluding holidays • Calls received after 5:00 PM local customer time (Monday - Friday) and/or dispatches submitted after that time may require an additional business day for a technician to arrive at customer's location

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 or migrated (ported) into your SDDC, as well as the physical environment and dependencies in your location for VMware Cloud on Dell racks.

Data Recovery

We will provide the following backup and recovery services:

- Management infrastructure including: vCenter Server, NSX Manager, Controller, and Edges, and all elements that make up the management stack.

You are responsible for the backup and recovery of the following:

- All application 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, service packs, and firmware updates related to the Service Offering.

Updates to the SDDC software and firmware are necessary to maintain the health and availability of the Service Offering, and are mandatory. These updates will be applied to your SDDC within the maintenance window provided by you and subject to the processes set forth in this section. You may not skip or delay application of these updates. However, VMware understands that sometimes you may need to delay or postpone maintenance on your system to accommodate critical business needs. In that case, you must contact VMware support at least 48 hours prior to the scheduled maintenance window to accommodate any changes you may require. VMware will work with you to facilitate changes to the scheduled maintenance window, while ensuring the application of these updates to maintain the health, stability and availability of the Service Offering.

We will provide notification of scheduled maintenance at least 24 hours in advance for any changes to the SDDC software and firmware that may impact your use of an SDDC. These changes may require downtime for SDDC management servers of up to eight hours per month for the SDDC. During this time, your workloads will typically continue to run unless there is a critical failure of hosts and the SDDC has to be shut down.

Restriction on Modification of System

The Service Offering hardware is a closed system, for use solely with the Service Offering. Customers are not allowed to physically interact with or modify the Service Offering hardware 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 your premises, you must not open or disturb the package containing the system, and keep the package in a safe location at your premises until a Dell-authorized 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 Service Offering hardware remains at all time in Dell. Dell retains all right, title and interest in and to the Service Offering hardware at all times, and the customer acquires no right or interest in the hardware by virtue of ordering a subscription to the Service Offering.

VMware reserves the right to replace the Service Offering hardware (with the assistance of Dell or a Dell-authorized technician) at a customer's location(s) at any time for any reason, consistent with the mutual agreement between VMware and Dell. VMware also reserves the right to reuse Service Offering hardware for different customers when appropriate. If we elect to provide previously deployed hardware to a customer, the hardware that is delivered will have all previous data and configurations deleted completely.

At VMware's discretion and consistent with the mutual agreement between VMware and Dell, Service Offering hardware may be refreshed by Dell or a Dell-authorized technician at the end of a customer's committed subscription term, depending on the length of the original subscription term and any renewal term. Service Offering hardware will not be refreshed during a committed subscription term. In the event of hardware refresh, VMware will assist the customer in migrating data and workloads to the new hardware.

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. This includes using Service Offering's hardware components such as the TPM (Trusted Platform Module) and leveraging root-of-trust mechanisms to verify Service Offering integrity.
- **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 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. 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. 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. This also includes the security of the physical network to which the Service Offering is connected.
- **Security Monitoring**: You are responsible for the detection, classification, and remediation of all security events associated with virtual machines, operating systems, applications, data or content that are isolated with your deployed SDDCs, 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 Service Offering Hardware:** You are responsible for ensuring the physical security of the Service Offering hardware at each installation location.
- **Insurance against damage, theft, and vandalism of the Service Offering Hardware:** You are responsible for purchasing insurance to adequately protect against physical risks that could damage or destroy the Service Offering hardware installed at your location; at a minimum, this must cover the replacement of the Service Offering hardware. 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 Service Termination, removing all sensitive data:** After the end of your subscription term, a Dell-authorized technician will retrieve the system from your premises. You are responsible for ensuring that Your Content has been removed from the system, within the time period specified in the decommission section below.

Business Operations

Billing

You will be billed for the entire committed term subscription in advance.There are no metered charges for use of the Service Offering. You can pay applicable charges for your subscription through redemption of VMware's Subscription Purchasing Program (SPP) credits or Hybrid

Purchasing Program (HPP) credits (collectively, “Credits”). Your Credit fund will be decremented for the entire subscription fee, upfront.

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

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 and service consoles.
- Virtual Machines deployed in your SDDC will be set to the “suspended” state and you will not be able to access or use them while your account is suspended.

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 will result in termination of your account, as provided in the Terms of Service.

Decommission of Service Offering Hardware

If you have elected to terminate your subscription at the end of your committed Subscription Term, you will have 45 days from the time we notify you within which to delete Your Content from the system. At the end of the 45 days, a Dell-authorized technician will remove the system from your premises. If you have not deleted Your Content from the system, it will be deleted by Dell.