VMware Cloud Disaster Recovery™

Service Description

Updated as of 15 May 2021

vmware

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.

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

1. Introduction

1.1 The Service Offering

VMware Cloud Disaster Recovery™ (the "Service Offering") can be used to protect your VMware vSphere® virtual machines by replicating them periodically to the cloud and recovering them as needed to a target VMware Cloud™ on AWS software defined data center ("SDDC"). The target SDDC can be created immediately prior to performing a recovery and does not need to be provisioned to support the replications in the Service Offering's steady state.

The Service Offering has the following components:

- DRaaS Connector – a virtual appliance installed in the customer's vSphere environment where the virtual machines to be protected are running under normal circumstances
- Scale-Out Cloud File System ("SCFS") – a cloud component that enables the efficient storage of backups of the protected virtual machines in cloud storage and allows virtual machines to be recovered very quickly without a time-consuming data rehydration process
- SaaS Orchestrator ("Orchestrator") – a cloud component that presents a user interface (UI) to consume the Service Offering and includes several disaster recovery orchestration capabilities to automate the disaster recovery process

1.2 Technical Documentation and Training

Public documentation covering key concepts, capabilities, deployment and configuration steps, administration procedures, and operational limits is available at https://vcdr.vmware.com/docs/index.html.

1.3 Legal Terms

Use of the Service Offering is subject to the Terms of Service, that can be found at the VMware end user terms landing page, at:
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

2. Service Operations

The following outlines VMware's roles and responsibilities in providing the Service Offering. While specific roles and responsibilities have also been identified as being owned by you, any roles or responsibilities not contained in this Service Description are either not the duty of VMware or are assumed to be your responsibility.

2.1 Service Provisioning

VMware will provide the following provisioning services:

- VMware will create an instance of the Service Offering for you when you request it from the Service Offering's landing page accessed via the VMware Cloud Services console at https://console.cloud.vmware.com. This instance of the Service Offering will include the SCFS, the Orchestrator, and other necessary cloud-based components. As part of the provisioning process, you will be contacted by VMware, using the contact information you

provide on the landing page, to confirm the particulars of the committed term subscription you want to purchase and the instance you want to deploy.
- VMware will create a corresponding Service Offering account and send an email or other notification to the contact information you provide on the Service Offering's landing page. Subsequently, you will be able to access the Service Offering's user interface by navigating to the VMware Cloud Services console and clicking on the tile corresponding to the Service Offering.
- VMware will ensure that the identified contact can create additional user accounts for other users, as needed.

Your responsibilities include:

- Installing and configuring the DRaaS Connector virtual appliance in the VMware vSphere environment where the virtual machines to be protected are running under normal circumstances.
- Ensuring the required network access from the DRaaS Connector virtual appliance to the cloud components of the Service Offering as specified in the documentation.
- Configuring the Service Offering to initialize protection of your virtual machines and prepare disaster recovery plans to facilitate recovery operations.

2.2 Support

For assistance in identifying and resolving errors, and to answer questions related to the operational use of the Service Offering, see the VMware Support Policies page, at https://www.vmware.com/support/policies.html.

In addition to any errors that you may encounter, VMware also proactively monitors for potential issues with your specific operational use of the Service Offering through an automated support capability built into the Service Offering. When a potential issue is identified that may require your intervention, VMware will proactively contact you to inform you about it and recommend actions that you can take to prevent or remediate it.

2.3 Incident and Problem Management

VMware will provide incident and problem management services (e.g., detection, severity classification, recording, escalation, and return to service) pertaining to:

- Infrastructure over which VMware has direct, administrative access and control, including servers and services used to provide the Service Offering.

You are responsible for incident and problem management (e.g., detection, severity classification, recording, escalation, and return to service) pertaining to:

- Your protection configuration, disaster recovery plan configuration, and other account settings in the Service Offering administrative management console.
- User-deployed and user-configured assets such as third-party tools and agents within the guest operating system of the protected virtual machines.
- Anything else not under VMware's direct control and administration.

2.4 Change Management

VMware will provide the following change management elements:

- Processes and procedures to maintain the health and availability of the Service Offering.

- Processes and procedures to release new code versions and bug fixes related to the Service Offering.

Updates to the Service Offering's component software – including the DRaaS Connector – are necessary to maintain the health and availability of the overall Service Offering and are mandatory. These updates will be applied to your instances of the Service Offering. 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 Service Offering software, VMware will not guarantee support for the affected instances.

You are responsible for:

- Management of changes to your protection configuration, disaster recovery plan configuration, alert settings, dashboards and other content.
- Administration of self-service features provided through the Service Offering's system console and user portal, up to the highest permission levels granted to you.
- Cooperating with VMware when planned or emergency maintenance is required.
- Ensuring that you do not modify the settings of the SDDC used for recovery of your virtual machines in a manner that disrupts the functionality of the Service Offering (e.g., changing the firewall configuration to interrupt access from the SDDC to the SCFS or Orchestrator components, attempting to unmount the Network File System ("NFS") datastores provisioned by the Service Offering, etc.). Please refer to this documentation page for guidance related to this: https://vcdr.vmware.com/docs/Content/vcdr/maintain-sddc-settings.htm

2.5 Restriction on Use

To facilitate quick recovery of the protected virtual machines to a VMware Cloud on AWS SDDC, the Service Offering automatically creates one or more NFS datastores and attaches them to the SDDC. Using these datastores, the recovery of the virtual machines can be initiated immediately, with the virtual disk backups still residing on the SCFS. The virtual machines can also run directly off these datastores – also referred to as the "Live Mount" – for a period of time while the virtual disk backup data is automatically copied in the background to the VMware vSAN™ datastore on the SDDC.

These NFS datastores are created exclusively for the purpose of exposing the virtual machine backups to the SDDC to facilitate disaster recovery and should never be used as general-purpose storage. You must not, and you are not permitted to, use the vSphere Client, vSphere APIs, or any method other than the interfaces provided by the Service Offering to create and power on virtual machines directly on these NFS datastores except through the capabilities and workflows exposed in the Service Offering. If this restriction is not adhered to, VMware will not guarantee support for the affected instances of the Service Offering.

2.6 Data Privacy

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 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.

2.7 Deletion of Data

Following expiration or termination of the Agreement, all Content, and all personal data contained in Content (other than Service operations data such as log files that may contain a server IP address, a machine name or details of Service configurations), in VMware's possession will be deleted from VMware's primary database and (if applicable) back-up database, as described in the "Termination" section, below. The only exception would be if and to the extent that VMware is required by applicable law to retain any of the personal data (in which case VMware will implement reasonable measures to isolate the personal data from any further processing). Service operations data will be deleted in accordance with the VMware Products & Services Privacy Notice, found at https://www.vmware.com/help/privacy/products-and-services-notice.html.

3. Business Operations

3.1 Billing and Usage Metering

Purchasing the Service Offering

The Service Offering is priced as a combination of two parts:

1. Per-TiB charge based on the sum of the logical storage size of the protected virtual machines and all the incremental cloud backups you choose to retain (where 1 TiB is equal to 2^40 bytes); and
2. Per virtual machine charge based on the number of protected virtual machines.

To use the Service Offering, you must purchase a committed term subscription for either a one-year or a three-year term for the per-TiB part (for a minimum quantity of five TiB). The per virtual machine part is always charged on an on-demand basis; that is, you are billed, in arrears, for the number of virtual machines protected.

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

Billing

For the per-TiB part of the Service Offering, you will be billed up front, in full, for the committed term subscriptions you purchase. Additionally you will be billed in arrears, at the applicable on-demand rates, for any metered usage in excess of your committed term subscriptions. The TiB usage metered every hour will be reduced by the quantity covered by the committed term subscriptions active in that hour, and the remainder usage amounts will be added across all hours in a month to determine the total monthly on-demand TiB usage.

For the per virtual machine portion, you will be billed in arrears, at the applicable on-demand rates, for all metered usage. The number of protected virtual machines will be metered every hour

and these metered amounts will be added across all hours in a month to determine the total monthly on-demand virtual machine usage. As of the date of this Service Description, we anticipate that this billing functionality (i.e., for the per virtual machine portion of the Service Offering) will be effective on or about April 15, 2021. We will notify you of the exact effective date prior to commencement of these charges becoming effective.

You will also be billed for any on-demand charges incurred through your use of VMware Cloud on AWS to recover your virtual machines. Refer to the VMware Cloud on AWS service description for additional information about billing and usage metering of VMware Cloud on AWS charges: https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/support/vmw-cloud-aws-service-description.pdf

You will not receive a separate bill from AWS for the underlying cloud infrastructure used by the Service Offering including cloud storage, cloud compute instances, managed databases, cloud network devices, and cloud management tools. These underlying cloud infrastructure components are included in the price of the Service Offering and you will not be billed separately for them by AWS or VMware.

After you have recovered your virtual machines into VMware Cloud on AWS SDDC, you may choose to use the "failback" capability included in the Service Offering to move your virtual machines back to your original protected site (once it becomes available for use again). To facilitate this failback in an efficient manner, the Service Offering transfers only the virtual machine data that has changed since the virtual machines were recovered into VMware Cloud on AWS. You will not receive a separate bill from AWS for the data transfer (i.e., egress) charges incurred in this process, and instead these charges will be borne by VMware. However, the amount of data transferred can become excessively large if there is a long delay between the recovery and the failback. VMware reserves the right to bill you for additional charges corresponding to excessive egress data transfers as part of a failback operation – defined as more than 50% of the protected virtual machine storage.

You must pay all applicable charges (both up-front charges for the committed term subscriptions and monthly on-demand charges) for the Service Offering through the redemption of VMware's Subscription Purchasing Program (SPP) credits. As you use the Service Offering, your SPP credit fund will be decremented, or charged, for your use of the services. If your SPP credit fund is depleted, the credit fund may go into an "overage" state and you will need to purchase additional SPP credits to true up the fund's negative balance. Refer to the following SPP Guide for information on SPP credits:

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

3.2 Host Capacity Needed for Disaster Recovery

The Service Offering does not include the VMware Cloud on AWS host capacity that is needed for disaster recovery testing or failover. You must separately purchase the VMware Cloud on AWS hosts you need to recover your protected virtual machines. You can purchase these hosts on an on-demand basis, or through committed term subscriptions, or a combination of the two. Refer to the VMware Cloud on AWS service description for additional information about purchasing VMware Cloud on AWS host capacity:

https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/support/vmw-cloud-aws-service-description.pdf

Note that the availability of VMware Cloud on AWS host capacity on an on-demand basis is not guaranteed, and will be considered on a best efforts basis. If you intend to purchase host capacity on an on-demand basis, contact your VMware sales representative to discuss your host capacity needs.

3.3 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. Consult your VMware sales representative for details on purchasing additional subscriptions. 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.

3.4 Termination

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. Your Content stored within the Service Offering will be permanently deleted within five to ten calendar days after the effective termination date and will not be recoverable after this.