VMware Cloud Disaster Recovery™

Service Description

Updated as of 17 August 2022
© 2022 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. This product is covered by one or more patents listed at http://www.vmware.com/download/patents.html.

VMware is a registered trademark or trademark of VMware, Inc. in the United States and/or other jurisdictions. All other marks and names mentioned in this Service Description may be trademarks of their respective companies.

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
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 (Disaster Recovery as a Service) Connector** – a software virtual appliance that must be installed in your vSphere environment where the virtual machines to be protected are running under normal circumstances
- **Scale-Out Cloud File System (“SCFS”)** – a hosted component of the Service Offering 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 hosted component of the Service Offering that presents a user interface (UI) to consume the Service Offering and includes several disaster recovery orchestration capabilities to automate the disaster recovery process. This is also known as the “Recovery Region” in the Global DR Console (as defined below).

The Service Offering also provides access to the following service consoles:

- **Global DR (Disaster Recovery) Console** – the user interface for provisioning Recovery Regions and creating subscriptions to the Service Offering.
- **VMware Cloud Console** (the “VMC Console”) – the user interface for provisioning SDDCs.

1.2 **Technical Documentation and Training**

Public documentation covering key concepts, capabilities, deployment and configuration steps, administration procedures, operational limits, and best practices is available at [https://docs.vmware.com/en/VMware-Cloud-Disaster-Recovery/index.html](https://docs.vmware.com/en/VMware-Cloud-Disaster-Recovery/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](https://www.vmware.com/download/eula.html)

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

You can provision the Service Offering using the Global DR Console. At minimum, you need one Orchestrator, one DRaaS Connector, and one SCFS. Additional instances can be added up to the supported maximum.

Your responsibilities during provisioning 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 hosted 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, please create a support request at


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 software components – 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. You may not, in the normal course, as VMware to skip or delay application of these updates. We will provide notification of scheduled maintenance at least 24 hours in advance for any changes that may impact your use of the Service Offering. Some updates to the Service Offering may be required for security, performance, availability, or stability reasons, including for issues that may affect all customers of the Service Offering. In most cases, a customer will be given a minimum of seven days’ notice for scheduled maintenance. VMware will use commercially reasonable efforts to provide 24 hours advance notice prior to any emergency maintenance. However, critical security vulnerabilities updates may be implemented by VMware with no advance notice. Customers may not refuse, or ask VMware to reschedule or postpone, emergency maintenance. VMware will take commercially reasonable steps to minimize emergency maintenance.

Your responsibilities with respect to change management include:

- 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:
  

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 Service Operations Data

In connection with providing the Service Offering, VMware collects and processes information from VMware’s software or systems hosting the Service Offering, and from your systems, applications, and devices that are used with the Service Offering, such as configuration, performance, and log data. 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.

2.7 Usage Data

The Service Offering collects data directly from VMware’s software or systems hosting the Service Offering, and from your systems, applications, and 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 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.

2.8 Deletion of Data

Upon termination of the Subscription Term, Your Content stored within the Service Offering will be permanently deleted five to 10 calendar days after the effective termination date and will not be recoverable after deletion. Also, all personal data associated with your use of the Service Offering will be deleted from VMware’s primary database and (if applicable) back-up database. The only exception will 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.

2.9 Service Location

The Service Offering is deployed in AWS data centers in multiple regions. You select the AWS region where your Orchestrator and SCFS instances will be deployed, and your backups and protection configuration will persist in that data center. VMware will not change the AWS region in which your Orchestrator and SCFS instances are deployed without your prior authorization. The Global DR Console data, including your term subscription 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.
2.10 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 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 to all VMware Cloud Disaster Recovery instances and VMware Cloud on AWS SDDCs that you deploy for recovery with the Service Offering.
- **Security Monitoring**: You are responsible for the detection, classification, and remediation of all security events that are isolated with your protected site, 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.

2.11 PCI Compliance

The Service Offering is certified as a PCI DSS Level 1 Service Provider, the highest level of assessment available. The compliance assessment was conducted by Crowe LLP, an independent Qualified Security Assessor (QSA). After initial deployment of the Service Offering, you must affirmatively take steps to configure your environment to meet your responsibilities as described in the Shared Responsibility Model, at: https://core.vmware.com/resource/vmware-cloud-disaster-recovery-shared-responsibility-model

You should make sure that the VMware Cloud on AWS SDDC used with Service Offering for recovering your virtual machines is PCI hardened, which might require disabling several VMware Cloud on AWS SDDC add-on capabilities in order to maintain compliance, including VMware HCX®. VMware will provide a customer-facing website, listing compliant offerings, that customers
can reference to ensure that they disable non-compliant VMC add-ons to maintain PCI compliance for their VMC on AWS environment. In addition, once a VMware Cloud on AWS SDDC is configured for PCI compliance, the networking and security configuration can be managed by you directly via the VMware NSX® Manager™ deployed in the SDDC rather than by the VMC Console.

For more details, refer to the documentation at docs.vmware.com. See the following for VMware Cloud on AWS Regions that are available for deployment of PCI compliant SDDCs: https://docs.vmware.com/en/VMware-Cloud-on-AWS/services/com.vmware.vmc-aws.getting-started/GUID-19FB6A08-B1DA-4A6F-88A3-50ED445CFFCF.html

Before deploying any other VMware service in your instance of the Service Offering, you should review the interoperability and compliance information for that other service. See https://cloud.vmware.com/trust-center/compliance for the most current information on compliant offerings. You are responsible for ensuring that any additional service deployed in your Service Offering instance meets your compliance and security requirements.

3. Business Operations

3.1 Billing and Usage Metering

Purchasing the Service Offering

The Service Offering is offered on an on-demand basis up to a maximum duration of six months, or you can purchase a committed term subscription. On-demand prices are charged hourly and billed monthly, and the Service Offering will be used in pilot mode. Pilot mode allows you to protect a capacity of 5 TiB and 25 virtual machines. If you exceed the amount of protected capacity or protected virtual machines, you will be charged overage fees on the amount exceeded at the then-current overage rate. There is no minimum period for which you need to run in pilot mode, but the pilot mode period may not exceed six months.

Committed term subscription pricing has 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.

A committed term subscription can be for either a one (1) year or three (3) year term for the per-TiB part (for a minimum quantity of 10 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.

Billing

For the per-TiB part of the Service Offering charges, you can elect to pay the committed charges either up-front (that is, all in advance) or in monthly installments. You will be billed in arrears, at the applicable on-demand rates, for any metered usage in excess of your committed capacity. The TiB usage metered every hour will be reduced by the quantity covered by the committed term subscriptions active in that hour, and the remaining 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 of the Service Offering charges, 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. You will also be billed for any on-demand charges incurred through your use of VMware Cloud on AWS to recover your virtual machines.

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 a 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 can pay all applicable charges (both charges for the committed term subscriptions and monthly on-demand charges) (i) through the redemption of VMware’s Subscription Purchasing Program (SPP) credits, (ii) by using a purchase order (PO) and invoice process, or (iii) or by credit card. If you elect to pay by redemption of SPP credits, 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: www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/solutions/vmware-spp-program-guide.pdf

If you elect to pay by using a credit card, you will be charged a nonrefundable fee of $2,000 USD or equivalent in your applicable non-USD currency, upon deployment of your first VMware Cloud on AWS SDDC. If, for any reason, the charge is rejected by your 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 towards your VMware Cloud on AWS SDDC. 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. You will be charged separately for VMware Cloud Disaster Recovery consumption in arrears every month, as they occur.

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. 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.
3.3 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, upon expiration of a committed subscription term, if you continue to use the Service Offering, 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 terminate your on-demand use.