FREQUENTLY ASKED QUESTIONS

VMware Cloud Disaster Recovery

Disaster Recovery as-a-Service

General

Q. What is VMware Cloud Disaster Recovery?

A. VMware Cloud Disaster Recovery is an easy-to-use, on-demand disaster recovery (DR) solution, delivered as SaaS, with cloud economics.

Q. What is the difference between VMware Cloud Disaster Recovery, VMware Site Recovery, and VMware Site Recovery Manager?

A. VMware Cloud Disaster Recovery is a Disaster Recovery as-a-service (DRaaS) solution that can be used to cost-effectively protect a broad set of your virtualized applications, with fast recovery capabilities. VMware Site Recovery is also a DRaaS solution that can be used to protect mission-critical applications that have a very low RPO and RTO. VMware Site Recovery Manager is an enterprise software solution, deployed and managed by you in your data center to facilitate DR protection to a secondary DR datacenter that you manage yourself

Q. How is VMware Cloud Disaster Recovery a cost-effective DRaaS solution?

A. There are three key ways in which VMware Cloud Disaster Recovery is cost-effective. First, you no longer need to own and continuously maintain a secondary DR site. Second, you can utilize an efficient cloud storage layer provided by the service to store your backups during the steady state and only consume failover compute and primary storage capacity when a disaster event occurs. Finally, this service provides an operationally consistent and familiar vSphere experience across the production and DR sites, so your IT staff doesn't need to learn new tools.

Q. What regions are currently supported?

A. The following regions are currently supported:

- US West (Oregon)
- US East (N. Virginia)
- US West (N. California)
- US East (Ohio)
- Canada (Central)
- Europe (Ireland)
- Europe (London)
- Europe (Frankfurt)
- Europe (Paris)
- Asia Pacific (Singapore)
- Asia Pacific (Mumbai)
- Asia Pacific (Sydney)
- Asia Pacific (Tokyo)

Getting Started

Q. How do I get started?

A. Getting started is easy. Simply reach out to us by going to VMware Cloud DR's *website* and clicking on "Get in touch".

Q. Do I need to learn new tools?

A. You use the same consistent, familiar vCenter management console and vSphere constructs on both your production and DR sites. For the DR service itself, you use an easy-to-use, SaaS-based management console.

Q. Do I need VMware Site Recovery to use VMware Cloud Disaster Recovery?

A. You do not need to enable VMware Site Recovery to use VMware Cloud Disaster Recovery.

Q. Do I need Site Recovery Manager (SRM) or vSphere Replication (VR) on my on-premises site to use VMware Cloud Disaster Recovery?

A. You do not need to deploy Site Recovery Manager (SRM) or vSphere Replication (VR) on your on-prem protected site to use VMware Cloud Disaster Recovery.

Q. What do I need to deploy on my source site?

A. You need to deploy one or more DRaaS Connector virtual machines in your on-premises vSphere environment to connect to the VMware Cloud Disaster Recovery components. DRaaS Connector is available as an easy-to-deploy OVA. You do not need to deploy any other appliance or hardware to connect to the VMware Cloud DR components in the cloud.

Q. Can I bring my own existing AWS account for VMware Cloud Disaster Recovery to use for the cloud storage?

A. The AWS account will be owned and managed by VMware, so you cannot bring your own AWS account.

Q. Can I setup Site Recovery Manager (SRM) style protection groups and recovery plans?

A. VMware Cloud Disaster Recovery supports grouping VMs into protection group as well as creating DR plans managed by its SaaS Orchestrator component, similar to Site Recovery Manager.

Protection groups can be based on VM names patterns or VM folder selection.

Q. Do I need a VMware Cloud on AWS SDDC in the steady state when I am only replicating to the cloud?

A. You do not need a VMware Cloud on AWS SDDC to be provisioned in the steady state. However, for customers that value low recovery times, we recommend a "pilot light" SDDC, which can currently be as small as a three host SDDC. Having a pilot light SDDC allows you to avoid the additional time needed to deploy an SDDC at the time of an outage and makes it possible to get alerts on the full set of automated DR health checks. Depending on your environment, it may also be helpful in pre-configuring the networking for your recovery SDDC and running foundational components such as Domain Controllers.

Q. Can I use the pilot light SDDC for running other VMs in the steady state, i.e. while I am only replicating?

A. Yes, the pilot light SDDC can be used for any purpose as it is a standard VMware Cloud on AWS SDDC in all respects.

Q. What are the bandwidth requirements with VMware Cloud Disaster Recovery?

A. The bandwidth required for replication would depend on the number, size, change rate, and RPO of the VMs that you are protecting. Upon recovery, you only need as much bandwidth to the cloud as is needed to communicate with your live workloads from your other sites and user endpoints.

Technical

Q. How does VMware Cloud Disaster Recovery work?

A. Using a simple, cloud-based UI you can configure backup policies protect your VMs and DR plans to orchestrate recovery of those VMs. Backups are encrypted and stored in the native vSphere VM format in a highly efficient cloud storage layer called the Scale-out Cloud File System (SCFS) instead of primary storage in a VMware Cloud on AWS SDDC. When disaster strikes, with a few clicks you can recover your VMs to VMware Cloud on AWS using your pre-tested DR plans. The service can be used to quickly provision VMware resources and SDDCs in VMware Cloud on AWS. The recovered VMs can be immediately powered-on using the stored backups via a "live mount", i.e. an NFS datastore automatically mounted to all hosts in that SDDC.

Q. How can I be sure that my disaster recovery plan will work when I need it?

A. DR health checks are automatically run every 30 minutes to increase your confidence that your DR plan will work when you need it.

Q. How do I achieve fast recovery times?

A. The "live mount" capability of VMware Cloud DR provides fast recovery without a time-consuming rehydration of the backup data from cloud storage to VMware Cloud on AWS hosts. The backed-up data is immediately made available in the recovery SDDC via an NFS datastore mounted to the SDDC hosts. Having a small deployment of pre-provisioned pilot light hosts makes the recovery process even faster.

Q. Does VMware Cloud Disaster Recovery convert the VMs to a different format for backup and recovery?

A. Unlike many other cloud-based data protection solutions, VMware Cloud DR keeps your protected VMs in their native vSphere VM format which eliminates the need for brittle VM conversions that slow down recovery and make failback error-prone.

Q. Does VMware Cloud Disaster Recovery support failback?

A. Yes, VMware Cloud DR supports an efficient, delta-based orchestrated failback back of the recovered VMs to your protected site when it becomes available again.

Q. How does failback work?

A. When you are ready, you can use the VMware Cloud DR management console to initiate failback. The changed data is compressed, encrypted, and automatically sent back to the original protected site.

Q. Does VMware Cloud Disaster Recovery support multiple backups for a single VM?

A. Yes, both VMware Site Recovery and VMware Cloud Disaster Recovery support the ability to retain multiple point-in-time snapshots for any protected VM. VMware Site Recovery allows you to retain up to 24 copies per VM. VMware Cloud DR allows you retain a large number of point-in-time snapshots for every VM. You can configure multiple schedules for each VM, and each schedule can have a different retention period.

Q. Can I recover from an older point-in-time snapshot?

A. You can recover from any point-in-time snapshot that is available based on your configured retention policies. Any of these snapshots – including the most recent one – can be used to immediately power-on your VMs, using the "live mount" capability.

Q. What storage options do you support for protection with VMware Cloud Disaster Recovery?

A. VMware Cloud DR supports the protection of vSphere VMs running on any vSphere compatible storage on a VMFS, NFS, or vSAN datastore.

Q. How does the DRaaS Connector get updated?

A. DRaaS Connector will be updated automatically and seamlessly without your intervention so that it stays compatible with the cloud service.

Support & Additional Resources

Q. How can I get support when using VMware Cloud Disaster Recovery?

A. You can contact VMware Support for any issues you face while using VMware Cloud DR.

Q. Where can I see a demo of VMware Cloud Disaster Recovery?

A. You can view pre-recorded demos *here*, which cover key VMware Cloud Disaster Recovery capabilities. Please reach out to your VMware Cloud Sales representative if you are interested in a live demo of the service.

Q. Is there a Hands-on-Lab that I can use?

A. A Hands-on-Lab for VMware Cloud Disaster Recovery is available in VMware HOL catalog *here*.

Q. Is there technical documentation available?

A. You can find the official technical documentation for VMware Cloud DR *here*.

Q. Where can I find operational limits for VMware Cloud DR?

A. You can find the operational limits for VMware Cloud DR *here*. Select "VMware Cloud Disaster Recovery" under "Select Product" and check all options under "All Categories" to view all the operational limits for VMware Cloud DR.

Q. Where can I find the datasheet for VMware Cloud Disaster Recovery?

A. You can find the datasheet for VMware Cloud Disaster Recovery *here*.

Q. What versions of other VMware software such as vCenter Server and ESXi work with VMware Cloud DR?

A. You can find the versions of VMware software that interop with VMware Cloud DR *here*.

Q. Where can I learn about the product roadmap for VMware Cloud Disaster Recovery?

A. The product roadmap for VMware Cloud DR is available under the "Disaster Recovery" category *here*.

Q. What service level agreement (SLA) do you offer for VMware Cloud Disaster Recovery?

A. Please refer to the Service Level Agreement document for VMware Cloud Disaster Recovery available *here.*

Q. Where can I find the terms and conditions for using VMware Cloud Disaster Recovery?

A. Please refer to the VMware Terms of Service for cloud service offerings, and the Service Description for VMware Cloud Disaster Recovery available *here.*

Q. Where can I find information about the most recent updates to VMware Cloud Disaster Recovery?

A. For information about the latest features and updates to the service, please refer to the release notes *here*.

Pricing

Q. Where can I find the price for VMware Cloud Disaster Recovery?

A. You can find the pricing for VMware Cloud Disaster Recovery on our *pricing page*.

Q. How can I purchase VMware Cloud Disaster Recovery?

A. Please refer to the "Business Operations" section of the Service Description for VMware Cloud Disaster Recovery available *here.*

Q. What currencies are supported for purchasing VMware Cloud Disaster Recovery?

A. The following six currencies are now supported for purchasing VMware Cloud Disaster Recovery: USD, GBP, EURO, JPY, AUD and CNY. You can transact in these currencies and protect your workloads in one of the AWS regions where VMware Cloud DR is available.

Q. How do I pay for VMware Cloud Disaster Recovery?

A. You pay for VMware Cloud Disaster Recovery service by redeeming SPP credits, including SPP credits specifically appliable to VMware Cloud on AWS. Refer to the *VMware Subscription Purchasing Program* guide for further information on SPP credits.

Q. When will I pay for VMware Cloud Disaster Recovery service?

A. Your SPP credits will be redeemed at the following points:

- When you purchase a 1-year or 3-year committed term subscription for the data capacity portion of the service, your credit fund will be decremented or charged upfront for the full amount of the one- or three-year subscription.
- Every month, your credit fund will be decremented or charged in arrears for any metered data capacity usage that exceeds your active committed term subscriptions.
- Every month, your credit fund will be decremented or charged in arrears for your metered protected VM count. Note that metering of protected VMs will be effective on or about April 15, 2021. Till that effective date, your credit fund will not be decremented or charged for the per-VM portion of the service.

For additional details about this, please refer to the "Billing and Usage Metering" section of the Service Description for VMware Cloud Disaster Recovery available *here.*

Q. Does the VMware Cloud Disaster Recovery pricing include VMware Cloud on AWS hosts?

A. No, you must separately purchase the VMware Cloud on AWS hosts required for DR testing and recovery of your protected VMs. VMware Cloud on AWS hots are not included in VMware Cloud Disaster Recovery pricing. More information about host pricing can be found on the *VMware Cloud on AWS pricing page*.

Q. Are there any other costs that I should be aware about?

A. The VMware Cloud DR price includes the underlying cloud infrastructure used by the service including cloud storage, cloud compute instances, managed databases, cloud network devices, and cloud management tools. Additionally, egress data charges incurred during typical use of the service for replication to the cloud and failback to the original protected site are also covered by VMware Cloud DR price. However, VMware reserves the right to bill you for additional charges corresponding to excessive egress data transfers.

Q. What do you consider excessive egress data transfers, for which I might be billed additional charges?

A. After you have recovered your virtual machines into a VMware Cloud on AWS SDDC, you may choose to use the failback capability to move your VMs back to your original protected site. To facilitate this failback in an efficient manner, VMware Cloud DR transfers only the VM data that has changed since the VMs were recovered into VMware Cloud on AWS. You will not receive a separate bill from AWS for the egress data transfer 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 or if none of the old data is available on the protected site anymore. 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 data capacity. The following rates apply to these excessive egress data transfer charges:

VMware Cloud on AWS region	Applicable rate per GiB* transferred
US East (N. Virginia)	$0.050
US East (Ohio)	$0.050
US West (N. California)	$0.050
US West (Oregon)	$0.050
Asia Pacific (Singapore)	$0.080
Asia Pacific (Mumbai)	$0.080
Asia Pacific (Sydney)	$0.092
Asia Pacific (Tokyo)	$0.084
Canada (Central)	$0.050
Europe (Frankfurt)	$0.050
Europe (London)	$0.050
Europe (Ireland)	$0.050
Europe (Paris)	$0.050

* 1 GiB equals 2^{30} bytes

Q. Does the VMware Cloud Disaster Recovery price include egress data transfers for VMs running on the recovery SDDC in VMware Cloud on AWS?

A. No, you will be separately charged for egress data transfers incurred by the recovered VMs when they are running in a VMware Cloud on AWS SDDC at the applicable VMware Cloud on AWS rates.Q. Is there a minimum purchase required for VMware Cloud Disaster Recovery?

A. Yes, you need to purchase at least 5 TiB of data capacity for a minimum 1-yr subscription. (1 TiB equals 2^{40} bytes)

Q. How is data capacity calculated?

A. Data capacity in TiB is calculated as the sum of the logical storage size of the protected VMs and all the incremental cloud backups you choose to retain (where 1 TiB is equal to 2^{40} or 1,099,511,627,776 bytes). For an accurate calculation of data capacity, please engage your VMware Cloud Sales representative.

Q. Can I co-term VMware Cloud Disaster Recovery subscriptions with VMware Cloud on AWS host subscriptions or VMware Site Recovery subscriptions?

A. No, co-terming capabilities are not available. You will have to manage the terms of the different subscription offerings.