

General Questions

Q. What has been announced?

A. VMware has announced the General Availability of VMware Cloud Disaster Recovery for Managed Service Providers. It will be available through VMware Cloud Partner Navigator on October 5, 2021. VMware Cloud DR will also be available through AWS Resell, which will allow partners to purchase it from Amazon Web Services and provision it for end customers through Cloud Partner Navigator.

Q. What is VMware Cloud Disaster Recovery?

A. VMware Cloud Disaster Recovery is an on-demand DR product, delivered as an easy-to-use SaaS solution, with cloud economics. It combines cost-efficient cloud storage with SaaS-based management to deliver IT resiliency at scale, through simple testing and orchestration of failover and fallback plans. Customers benefit from a 'pay when you need' failover capacity model for DR resources. VMware Cloud Disaster Recovery enables partners to help customers optimally assess and balance their technical capabilities in the cloud, strengthening business resilience in the face of data loss threats such as ransomware whilst making the process more time and cost efficient.

Q. How can partners leverage VMware Cloud Disaster Recovery as an MSP offering?

A. Partners can leverage the benefits of VMware Cloud Disaster Recovery to offer customers an end-to-end VMware DRaaS solution that is tightly integrated with VMware Cloud on AWS, delivers fast recovery times, low Recovery Point Objective (RPOs), and leverages cloud economics to deliver low total cost of ownership.

Q. How does VMware Cloud Disaster Recovery add value to partners?

A. Partners can accelerate and operationalize their customer's DR journey by offering professional services to plan, define, configure, test and operate a VMware Cloud DR-based design, improving their customer relationships by addressing this critical business resiliency need.

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

A. VMware Cloud Disaster Recovery is an on-demand Disaster Recovery as-a-service (DRaaS) solution that can be used to cost-effectively protect a broad set of virtualized applications, with fast recovery capabilities and lower total cost of ownership than with traditional DR. VMware Site Recovery is also a DRaaS solution that requires maintenance of full failover capacity in the cloud (vs. the on-demand capability that VMware Cloud DR

offers). It can be used to protect mission-critical applications that have a very low Recovery Point Objective (RPO) and Recovery Time Objective (RTO). VMware Site Recovery Manager is a traditional DR enterprise software solution, deployed and managed by the customer in their data center to facilitate DR protection to a secondary DR datacenter, also customer-managed.

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, customers no longer need to own and continuously maintain a secondary DR site. Second, they can utilize an efficient cloud storage layer provided by the service to store their 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 the partner's IT staff doesn't need to learn new tools.

Q. What are the main use cases for VMware Cloud Disaster Recovery?

- A. **1. Replace Existing DR:** Partners can help customers accelerate cloud adoption by modernizing DR infrastructure. They can offer faster DR with on-demand failover capacity that eliminates the need to maintain a secondary DR site.
- 2. Optimize DR Costs:** Partners can help customers maximize ROI through a tiered approach to DR - optimizing DR costs by tuning SLAs and TCO to match application requirements.
- 3. Accelerate Ransomware Recovery:** Partners can ensure confident recovery from ransomware with a plan that runs rapid recovery point validations, restores critical applications and supports a resiliency strategy.

Q. What regions are currently supported for VMware Cloud Disaster Recovery?

A. For an updated list of regions, please refer to the [product FAQ](#):

- US East (N. Virginia)
- US East (Ohio)
- US West (N. California)
- US West (Oregon)
- Canada (Central)
- S. America (Sao Paulo)
- Europe (Milan)
- Europe (Paris)
- Europe (Stockholm)
- Asia Pacific (Mumbai)
- Asia Pacific (Seoul)
- Asia Pacific (Singapore)

- Europe (Frankfurt)
- Europe (Ireland)
- Europe (London)
- Asia Pacific (Sydney)
- Asia Pacific (Tokyo)

Getting Started

Q. How do partners get started?

A. Partners can find an aggregator [here](#) or contact their sales representative.

Q. How can partners learn more about VMware Cloud Disaster Recovery before purchasing the service?

A. Partners can learn more about VMware Cloud Disaster Recovery by accessing the MSP [webpage](#), product [webpage](#), product [HOL](#) or reaching out to a sales representative.

Q. Do partners need to learn new tools?

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

Q. Is there any training requirement for VMware Cloud Disaster Recovery?

A. No training is required for VMware Cloud Disaster Recovery but needs to be done for VMware Cloud on AWS.

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

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

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

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

Q. What do partners need to deploy on their source site?

A. Partners need to deploy one or more DRaaS connector virtual machines on their source site vSphere environment to connect to the VMware Cloud Disaster Recovery components. DRaaS connector is available as an easy-to-deploy OVA. They do not need to deploy any other appliance or hardware to connect to the VMware Cloud DR components in the cloud.

Q. Can partners bring their 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 partners cannot bring their own AWS account.

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

A. VMware Cloud Disaster Recovery supports grouping VMs into protection groups as well as creating DR plans managed by its SaaS Orchestrator component, similar to Site Recovery Manager. Protection groups can be based on VM name patterns or VM folder selection.

Technical Questions

Q. How does VMware Cloud Disaster Recovery work?

A. Using a simple cloud-based UI, partners can configure backup policies to protect their 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 they can recover the VMs to VMware Cloud on AWS using their 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 partners be sure that the disaster recovery plan will work when it is needed?

A. DR health checks are automatically run every 30 minutes to increase confidence that the DR plan will work when it is needed.

Q. How do partners achieve fast recovery times?

A. The “live mount” capability of VMware Cloud Disaster Recovery 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 Disaster Recovery keeps protected VMs in the 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 Disaster Recovery supports an efficient, delta-based orchestrated failback of the recovered VMs to the protected site when it becomes available again.

Q. How does failback work?

A. When partners are ready, they can use the VMware Cloud Disaster Recovery 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 Disaster Recovery allows partners to retain up to 2000 snapshots per protection group. They can configure multiple schedules for each VM, and each schedule can have a different retention period.

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

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

Q. What storage options are supported for protection with VMware Cloud Disaster Recovery?

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

Q. How does the DRaaS connector get updated?

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

Support & Additional Resources

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

A. MSPs are responsible for support for their customers. All service incidents and supporting tickets can be routed via the Cloud Partner Navigator, where the service is managed.

For product, technical, and non-technical support related to VMware Cloud DR, partners can (1) Open a support ticket via the support center of the Cloud Partner Navigator platform or (2) Use the chat functionality in the

console or (3) Call us. Support ticket is the most preferable method to contact us.

For contract, usage, billing, additional license order related support, partners can raise a ticket within the commerce portal.

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

A. Partners can view pre-recorded demos [here](#), which cover key VMware Cloud Disaster Recovery capabilities. Partners can reach out to their VMware cloud sales representative if they are interested in a live demo of the service.

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

A. A Hands-on-Lab for VMware Cloud Disaster Recovery is available in the VMware HOL catalog [here](#).

Q. Is there technical documentation available?

A. Partners can find the official technical documentation for VMware Cloud Disaster Recovery [here](#).

Q. Where can partners find operational limits for VMware Cloud Disaster Recovery?

A. Partners can find the operational limits for VMware Cloud Disaster Recovery [here](#). They can select “VMware Cloud Disaster Recovery” under “Select Product” and check all options under “All Categories” to view all the operational limits for VMware Cloud Disaster Recovery.

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

A. Partners can find the versions of VMware software that interop with VMware Cloud Disaster Recovery [here](#).

Q. What Service Level Agreement (SLA) is offered for VMware Cloud Disaster Recovery?

A. Please refer to the Service Level Agreement document for VMware Cloud Disaster Recovery available [here](#).

Q. Where can partners 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](#).

Commercial Questions

Q. How will partners get billed for the consumption of the service?

A. Partners who have MSP commit contracts must validate usage in the corresponding Monthly Billing Order (MBO) in the Commerce Portal by the **10th day** of every month and



submit the report to the Aggregator by the **15th day** of the month, who will invoice the cloud provider.

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

A. Partners can find the details in the [pricing handbook](#). Please reach out to AWS for the pricing for AWS Resell route.

Q. How can partners purchase VMware Cloud Disaster Recovery?

A. The cloud provider must have a **VMware Cloud on AWS commit contract** in place and the SDDC enabled before they can purchase VMware Cloud Disaster Recovery at this time. VMware Cloud Disaster Recovery is also provided under a commit contract which the cloud provider must sign with a VMware Aggregator. The commit contract covers a currency cash commit which is discounted the more partners commit to and longer the term. Or a cloud provider can use their existing rental point level to discount the MSRP and then apply a term for further discount. Specific discount and commit tiers are available in the [pricing handbook](#) on Partner Connect or from their Aggregator.

Q. Who can buy VMware Cloud Disaster Recovery?

A. Only VMware cloud providers who have signed up for the MSP agreement and have a VMware Cloud on AWS commit contract can purchase VMware Cloud Disaster Recovery service. Service providers must have both a VMware Cloud on AWS commit contract and a VMware Cloud Disaster Recovery commit contract in place.

Q. Does VMware provide leads or sales incentives to cloud providers?

A. No, VMware does not provide leads or sales incentives to cloud providers. Cloud providers are expected to generate their own pipeline and market their own services on the platform.

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

A. Partners will be charged for the service at the following points:

- When they purchase a 1-year or 3-year committed term subscription for the data capacity portion of the service, they will be charged upfront for the full amount of the one- or three-year subscription. They can also choose to pay monthly for the one- or three-year subscription, in which case they will be charged every month until the end of their subscription term.
- Every month, they will be charged in arrears for any metered data capacity usage that exceeds their active committed term subscriptions.

Q. Can partners try out the service before committing to a long-term subscription?

A. A paid pilot is available for partners that is metered hourly and billed monthly. Please reach out to your aggregator or sales representative for details and note the below restrictions for the pilot:

- The pilot offers 5 TiB capacity and up to 25 VMs to protect. Additional charges are applied if these numbers are exceeded.
- The pilot cannot be used for longer than 6 contiguous months
- The paid pilot automatically ends when the first term subscription is created in the same geo
- Only one paid pilot per org is available at a time (single one across all regions)

Q. Can a partner get a paid pilot for every customer org?

A. Yes, the partner can get a paid pilot for every customer org.

Q. How can the pilot be disabled?

A. The paid pilot is terminated when the customer purchases a new subscription. For other cases, please consult your VMware sales representative.

Q. If the customer purchases VMware Cloud on AWS directly, can that SDDC be used as a DR site with a cloud provider org in Cloud Partner Navigator?

A. Both VMware Cloud Disaster Recovery and VMware Cloud on AWS need to be enabled in the same organization.

Q. Does the paid pilot offer the full feature set of VMware Cloud Disaster Recovery?

A. Yes, there is no limitation to the functionality of the product.

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

A. No, partners must separately purchase the VMware Cloud on AWS hosts required for DR testing and recovery of the protected VMs. VMware Cloud on AWS hosts 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 partners should be aware of?

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 over the internet are also covered by VMware Cloud DR price. However, VMware reserves the right to bill partners for additional charges corresponding to excessive egress data transfers. If partners choose to failback to the original protected site using Public VIF over AWS Direct Connect, they will incur egress charges which are not covered by VMware. Refer to [AWS Direct Connect documentation](#) for pricing information.

Q. What are considered excessive egress data transfers, for which partners might be billed additional charges?

A. After partners have recovered the customer virtual machines into a VMware Cloud on AWS SDDC, they may choose to use the failback capability to move their VMs back to the original protected site. To facilitate this failback in an efficient manner, VMware Cloud Disaster Recovery transfers only the VM data that has changed since the VMs were recovered into VMware Cloud on AWS. Partners will not receive a separate bill from AWS for the egress data transfer charges over the internet 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 partners 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. Do note that egress data transfer charges using AWS Direct Connect over Public VIF are not borne by VMware, and partners would receive a separate bill from AWS for those if incurred. The following rates apply to these excessive egress data transfer over the internet:

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
Asia Pacific (Seoul)	\$0.108
Canada (Central)	\$0.050
South America (Sao Paulo)	\$0.114
Europe (Frankfurt)	\$0.050
Europe (London)	\$0.050
Europe (Ireland)	\$0.050
Europe (Paris)	\$0.050
Europe (Stockholm)	\$0.050
Europe (Milan)	\$0.050

* 1 GiB equals 2³⁰ 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, partners 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. There is no minimum purchase requirement for MSPs. However, VMware Cloud Disaster Recovery has a minimum purchase of 10 TiB and 1- or 3- year subscription.

VMware Cloud Disaster Recovery is priced as a combination of a per-TiB charge based on the protected storage capacity and a per virtual machine charge based on the number of protected VMs (total price = \$/TiB + \$/VM). To use the offering, partners must purchase a committed term subscription for either a 1- or 3-year term for the per-TiB part (for a minimum quantity of 10 TiB). Please refer to the details [here](#).

[VMware Cloud Disaster Recovery on Cloud Partner Navigator](#)

Q: How can cloud providers transact with VMware Cloud Disaster Recovery?

A: VMware cloud providers must use the Managed Service Provider (MSP) lifecycle to transact with the service:

- **Commit Contract** – Partner signs a VMware Cloud Disaster Recovery Managed Service Provider commit contract with a VMware Aggregator. Partner then commits to VMware an MSRP (list price) spend to obtain a volume discount for their purchases.
- **Cloud Provider Builds Pipeline** – Partner initiates go to market activities and starts building their business for Managed Services.
- **Deliver Managed Services and Own the Terms of Service** – Once the opportunity has been identified, partners can order VMware Cloud Disaster Recovery from VMware and provide Managed Services as part of the offering to their customers. Partners must provide their own terms of service and managed services. At a minimum this must include technical support for the service and all functions associated with service configuration, add-ons, renewals and anything pertaining to billing.
- **On-Board and Provide Support to their Customers** – Partner will on-board VMware Cloud Disaster Recovery for their customers. Subsequently, they may obtain technical support from VMware as needed, with the following [provisions](#). In turn, partners are responsible for all customer support, which may include, but may not be limited to customer communication, any managed services, answering installation, configuration and usage questions.
- **Complete Monthly End Customer Reports and Pay Invoices** – The partner will log into the Commerce Portal



and review the prior month's usage. They can view their Monthly Billing Orders (MBOs) in the Monthly Reporting menu. Partner will review the report and submit it to their Aggregator. Following that, the Aggregator will send the partner an invoice for the month.

Q. How can partners onboard the service tile for VMware Cloud Disaster Recovery on VMware Cloud Partner Navigator?

A. Before onboarding, MSPs must have at least one active commit contract in the Commerce Portal for an available service, a valid VMware ID associated with an active commit contract and the provider org invitation email. They can work with an Aggregator to sign a commit contract for VMware Cloud Disaster Recovery, which will be set up in the VMware Commerce Portal. Once the commit contract becomes active in the commerce portal, the partner will receive an on-boarding invitation email and a corresponding tile is made available under 'Services Available for provisioning' on Cloud Partner Navigator. Selecting open on the tile will activate the service and it will be available under 'Services provisioned for you'. For details, partners can refer to the [Cloud Partner Navigator](#) documentation.

Q. Is the provider org creation process same as that of other services on Cloud Partner Navigator?

A. Yes, partners can follow the same process for creating a provider org for VMware Cloud Disaster Recovery. If they have already onboarded to the provider organization using another MSP commit contract, when the MSP VMware Cloud Disaster Recovery commit contract becomes active in the commerce portal, it will be available under 'Services available for provisioning'. Please review the 'Creation of Provider Org' in the online documentation [here](#).

Q. How does the customer creation and management process work for VMware Cloud Disaster Recovery?

A. Before MSPs can start provisioning and managing services for their customers, they must first create a customer organization for them. They must have a valid VMware ID account for the email used to create the commit contract, an on-boarded provider org, and a valid VMware ID for the customer admin. For step by step instructions on creating a customer organization, partners can refer to the online documentation [here](#).

Q. Can the MSP control the level of access that the customers receive?

A. Yes, all customer users in Cloud Partner Navigator hold a role within their organization, which defines the range of activities they can perform within it. Consult the [Cloud Partner Navigator documentation](#) or our [operations handbook](#) for more details on the different user roles available. The access is defined on an organizational level, so all users in that organization will have that access. Providers should NOT grant "SDDC Admin" or "Administrator" roles in VMware Cloud Disaster

Recovery if they don't want the customer to create/modify the recovery of SDDCs themselves.

Q. How can MSPs manage the usage consumption and billing for their end customers?

A. Bills are spooled in the VMware Cloud Provider Commerce Portal in monthly arrears and VMware Cloud Disaster Recovery commit contract usage information can be viewed in the Commerce Portal > Monthly Reporting > Select filters from displayed Monthly Billing orders (MBOs) > View Details > Provide PO number > Submit/ Download.

Usage chargeback for customers can be viewed and managed via the Cloud Partner Navigator platform. For further details on this functionality, read this [blog](#).

Business Operations

Q. How do MSPs get started with VMware Cloud Disaster Recovery?

A. Refer to the MSP [Operations Handbook](#), the VMware Cloud Disaster Recovery Solution Brief, the [Getting started](#) with Cloud Partner Navigator or [Using Cloud Partner Navigator](#) documentation. MSPs can also refer to the resources on our MSP [webpage](#), and access the Navigator [Partner Connect page](#), VMware Cloud DR [product page](#), VMware Cloud DR [tech zone](#) or the VMware Cloud DR [product FAQ](#).

Q. What is the billing frequency?

A. The billing frequency is monthly.

Q. What are the reporting requirements for VMware Cloud Disaster Recovery?

A. Once a month, partners need to complete reporting inside the VMware Commerce Portal. All the service information will be pre-populated with the information that MSPs entered while ordering. This report is used to initiate the monthly billing cycle. You can refer to [this](#) blog or [this](#) documentation to learn more about the Commerce Portal.

Q. What are the timelines for monthly reporting?

A. Partners who have MSP commit contracts must validate usage in the corresponding Monthly Billing Order on the Commerce Portal by the [10th day](#) of every month and submit the report to the Aggregator by the [15th](#).

Q. How can partners demo VMware Cloud Disaster Recovery?

A. Leverage the [Hands on Labs](#) (HOL) environment.