



# VMware Cloud Disaster Recovery as a Service Standard

## For VMware Cloud on AWS

### At a glance

VMware Cloud Disaster Recovery as a Service (DRaaS) Standard offer a fast-track to help you create a recovery site, build a disaster recovery plan, and protect your workloads and apps to VMware Cloud on AWS.

### Key benefits

- Rapid setup of your recovery site
- Identification of apps and creation of their protection group
- Creation of a disaster recovery plans
- Learn from experts using a proven methodology and best practice

### SKU

PS-CLD-DRAAS-STD-C

### Service overview

VMware Cloud™ Disaster Recovery as a Service for VMware Cloud on AWS provides a rapid setup of a recovery site, creation of protection groups of VMs associated with applications to be protected and the creation of a disaster recovery plan using VMware Cloud Disaster Recovery™ or VMware Site Recovery™. To ensure your team is fully enabled we will guide you through the process and we will have a knowledge transfer session focused on to your needs.

The following activities are included in this service:

- Activation in one (1) recovery site of either VMware Cloud Disaster Recovery or VMware Site Recovery on VMware Cloud on AWS
- Activation in one (1) protected site of either VMware Cloud Disaster Recovery or VMware Site Recovery, on-premises or on VMware Cloud on AWS
- Creation of up to seven (7) protection group for up to thirty-five (35) VMs in total
- Creation of up to two (2) disaster recovery plans
- Test of the created disaster recovery plans
- A knowledge transfer session about VMware Cloud Disaster Recovery or VMware Site Recovery

This service requires the following VMware products, with vendor-supported versions as agreed to by VMware and Customer at project kickoff, but limited to those that are in general availability (GA) on the date of service purchase:

- VMware Cloud Disaster Recovery **OR** VMware Site Recovery
- VMware Cloud on AWS
- VMware vCenter® 6.5 or higher (\*)

(\*) Please check the VMware products requirements and interoperability matrix links in the Appendix.

### Service delivery description

Service activities will be entirely delivered remotely by VMware Professional Services offshore resources. Due to the nature of some on-premises components and security aspects we require Customer to join virtual sessions

and engage their infrastructure, network and security teams when appropriate to execute required actions (i.e., firewall port configurations or appliance deployments) under VMware team supervision. The delivery team will also require validating the proper configurations and requirements are in place before proceeding with the remote installation.

### Service capabilities

This service contributes to the development of the following capabilities:

- Replicate and protect workloads into VMware Cloud
- Recover from data center outages
- Project scope
- This service covers only one (1) product, VMware Cloud Disaster Recovery or VMware Site Recovery, chosen by the Customer with the specific scope defined in the following tables.

VMware Cloud Disaster Recovery		
Specification	Parameters	Description
VMware Cloud Disaster Recovery Pilot light	Up to one (1)	VMware Cloud Disaster Recovery Pilot light SDDC to be deployed.
VMware Cloud Disaster Recovery On-premises sites	Up to one (1)	VMware Cloud Disaster Recovery on-premises appliance be installed and configured in the service deployment.
Protection groups	Up to seven (7)	VMware Cloud Disaster Recovery protection group(s) configured.
Disaster Recovery plans	Up to two (2)	VMware Cloud Disaster Recovery DR plan configured.
DR Plan testing and cleanup	Up to two (2)	Test and cleanup for a recovery plan consisting of up to five (5) VMs and up to 200GB each VM.

VMware Site Recovery		
Specification	Parameters	Description
VMware Site Recovery Add-on for VMware Cloud on AWS	Up to one (1)	VMware Site Recovery to be activated and configured in the VMware Cloud on AWS SDDC

VMware Site Recovery on-premises appliances	Up to one (1)	On-premises components: one (1) VMware vSphere® replication appliance and one (1) VMware Site Recovery Manager appliance deployed in Customer environment.
Protection groups	Up to seven (7)	Site Recovery Manager Server protection group(s) configured.
Recovery plans	Up to two (2)	Site Recovery Manager Server Recovery plan(s) configured.
Recovery Plan testing and cleanup	Up to two (2)	Test and cleanup for a recovery plan consisting of up to five (5) VMs and up to 200GB each VM.

Protect workloads		
Specification	Parameters	Description
Protection groups	Up to seven (7)	Protection groups to be designed and configured.
Virtual Machines (VMs) protected	Up to thirty-five (35)	VMs to be protected.

## Out of scope

The following are out of scope items for this project.

### General

- Installation and configuration of custom or third-party applications and operating systems on deployed virtual machines
- Operating system administration including the operating system itself or any operating system features or components
- Management of change to virtual machines, operating systems, custom or third-party applications, databases, and administration of general network changes within Customer control
- Remediation work associated with any problems resulting from the content, completeness, accuracy, and consistency of any data, materials, or information supplied by Customer
- Installation or configuration of VMware products not included in the scope of this document
- Installation and configuration of third-party software or other technical services that are not applicable to VMware components
- Installation and configuration of Customer-signed certificates

- Configuration of VMware products used for the service other than those implemented for the mutually agreed-to use cases
- Customer solution training other than the defined knowledge transfer session

### **VMware Cloud on AWS**

- Creation of VMware Cloud Organization
- Creation and configuration of SDDC(s) and Clusters
- Creation and configuration of the required AWS Account
- VPNs and network connectivity configurations
- Creation of user roles and groups
- Creation of local accounts
- Configuration of LDAP/Active Directory sources
- Creation of Networking segments, VPNs, and additional firewall rules not defined by the specific service scope
- Design or configuration of interconnectivity between different SDDCs or other native cloud services

### **VMware Cloud Disaster Recovery**

- Creation and configuration of the required AWS Account
- On-premises networking and firewall configuration is customer responsibility
- VMware Site Recovery and VMware Cloud Disaster Recovery do not support protecting the same VMs on the same DR target SDDC; VMware Cloud Disaster Recovery will not be able to failover VMs protected by VSR on the same DR target SDDC
- VMs created by vSphere vApp(s) are not supported
- Fault Tolerant VMs are not supported
- VMs with Shared disks are not supported

### **VMware Site Recovery**

- Creation and configuration of the required AWS Account
- On-premises networking and firewall configuration is customer responsibility
- VMware Site Recovery and VMware Cloud Disaster Recovery do not support protecting the same VMs on the same DR target SDDC; VMware Cloud Disaster Recovery will not be able to failover VMs protected by VSR on the same DR target SDDC
- VMs created by vSphere vApp(s) are not supported
- Fault Tolerant VMs are not supported
- VMs with Shared disks are not supported

### Workload protection

- Pre- and post-application DR validation
- Backup/restore of virtual machines
- Virtual machines with raw device mappings (RDM) in physical compatibility mode
- Virtual machines with SCSI bus sharing
- VMware NSX® security tags and configurations of security groups and policies related to the virtual machine.
- Physical servers to virtual machines conversions
- Clustered virtual machines

### Estimated schedule

VMware estimates that the duration of this project will not exceed 3 weeks. VMware will operate according to a schedule agreed to by both parties. Typically, services are performed during normal business hours and workdays (weekdays and non-holidays).

### Project activities

#### Phase 1: Initiate

VMware hosts a project initiation call with key Customer and VMware stakeholders.

Topics to be discussed include:

- Project business drivers, scope, and objectives
- Project deadlines, timelines, scheduling, and logistics
- Identification of key Customer team members who VMware will work with to accomplish the tasks defined in this data sheet
- Technology prerequisites necessary for a successful project, including review of the Service Checklist for the VMware solution
- Confirmation of team members and contact details will be exchanged to schedule the project kickoff meeting

Deliverables include:

- Initial pre-engagement call

#### Phase 2: Plan

VMware leads a project kickoff meeting with Customer to assess prerequisite completion readiness, review the VMware standard architecture, and confirm project milestone dates.

The objectives of the meeting are as follows:

- Introducing the VMware team, roles, and responsibilities

- Describing the project goals, phases, and key dates
- Explaining the expected project results and deliverables
- Agreeing on communication and reporting process
- Validating the project expectations and clarifying roles and responsibilities

After Customer and VMware agree on project expectations, the VMware Project Manager and the Customer Project Manager work together on the detailed project plan.

Deliverables include:

- Project kickoff meeting minutes
- VMware Cloud Disaster Recovery or VMware Site Recovery kickoff presentation
- list of VMs to be protected

### **Phase 3: Execute**

The key activities for this phase are organized into Deploy and Knowledge Transfer subphases.

In the Deploy subphase VMware deploys, documents, and validates the technology components according to the specifics. VMware does the following:

- Installs and configures the VMware technologies according to the specifications
- Finalizes the Configuration Workbook
- Collection and validation the VMs to be protected
- Creation of Protection group(s)
- Creation of DR Plan(s) for VMware Cloud Disaster Recovery or recovery plan(s) for VMware Site Recovery
- DR Plan(s) for VMware Cloud Disaster Recovery or recovery plan(s) for VMware Site Recovery testing activities

Deliverables include:

- Solution specification workbook
- Solution verification workbook
- Knowledge Transfer workshops up to four (4) Hrs.

### **Phase 4: Close**

VMware conducts a closure meeting of up to two (2) hours with the Customer covering project status, reviewing completions, next steps and how to engage with VMware support.

## Learn more

Visit [vmware.com/services](https://vmware.com/services).

## Appendix

### Service checklist

The following Customer stakeholders are required to deliver this service:

- VMware operations team leads
- Application operations leads
- Security policy team leads
- Enterprise Architect
- Infrastructure Architect
- Network Operations team leads
- Network Architecture team leads

### Product compatibility matrix

Please verify the on-premises version of your vCenter and vSphere components using the VMware product compatibility matrix for [VMware Cloud Disaster Recovery](#) or [VMware Site Recovery](#).

### Important requirements

For VMware Site Recovery, an SDDC must be already available and configured to enable the VMware Site Recovery add-on. VMware Cloud Activation™ services can set up the SDDC if help is needed.

Please read the [VMware Cloud Disaster Recovery Release Notes](#) and [VMware Site Recovery Release Notes](#) for the full list of requirements and limitations.

This service must be delivered and accepted within the first 12 months of purchase, or the service will be forfeited. Pricing for this service excludes travel and other expenses. For detailed pricing, contact your local VMware representative.