



# VMware Cloud Disaster Recovery as a Service Standard

## for Azure VMware Solution

### At a glance

VMware Cloud Disaster Recovery as a Service (DRaaS) Standard offers a fast-track to build a disaster recovery solution and protect your workloads and applications to Azure VMware Solution using VMware Site Recovery Manager.

### Key benefits

- Implement a comprehensive DR strategy quickly and efficiently
- Rapidly setup your recovery site
- Simplify DR operations
- Establish ongoing processes to validate DR plans and remove configuration drift
- Meet your RPO and RTO goals
- Learn from experts using proven methodology and best practice

### SKU

PS-AVS-DRAAS-STD-C

### Service overview

VMware Cloud™ Disaster Recovery as a Service for Azure VMware® Solution provides rapid setup of a recovery site to protect VMs, definition and creations of protection groups, and the configuration of disaster recovery plans using VMware Site Recovery Manager™. 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.

### Service delivery description and requirements

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.

The following activities are included in this service:

- Support for the activation in one (1) recovery site in Azure VMware Solution of Site Recovery Manager components.
- Support for the activation in one (1) protected site of Site Recovery Manager in Azure VMware Solution or deployment of Site Recovery Manager appliances in one (1) on-premises vSphere environment
- 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 Site Recovery Manager

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:

- Site Recovery Manager 8.3.1 or higher
- Azure VMware Solution 2.0 or higher
- VMware vCenter® 6.5 or higher (\*)

(\*) Note 1: Please check the VMware products requirements and interoperability matrix links in the Appendix.

## Project scope

This service contributes to the development of the following capabilities:

- Replicate and protect workloads into Azure VMware Solution
- Recover from data center outages

A specific set of scope parameters are defined in the following tables:

VMware Site Recovery Manager		
Specification	Parameters	Description
Site Recovery Manager for Azure VMware Solution	Up to one (1) Recovery site	Site Recovery Manager to be activated and configured as the recovery Azure VMware Solution
Site Recovery Manager on-premises or Azure VMware Solution	Up to one (1) Protected site	Azure VMware Solution or on-premises components: one (1) VMware vSphere® replication appliance and one (1) 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.

Protected 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 service divided by section.

### 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
- Customer solution training other than the defined knowledge transfer session

### Azure VMware Solution

- Creation of the VMware software-defined data center (SDDC) in Azure VMware Solution
- Creation and configuration of SDDC(s) and Clusters
- 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

### Site Recovery Manager

- Configuration of On-premises networking and firewall
- Protection of VMs created by vSphere vApp(s)
- Protection of Fault Tolerant VMs
- Protection of VMs with Shared disks
- Replication using Array-based, VVOLs, and storage policy Protection Groups

## 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
- Site Recovery Manager presentation
- Collected 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
- Review and validation of the VMs to be protected
- Creation of Protection group(s)
- Creation of recovery plan(s) for Site Recovery Manager
- testing activities for the recovery plan(s)

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 going forward.

## 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 and interoperability matrix

Please verify VMware product compatibility and interoperability matrix for:

- [Site Recovery Manager](#)
- [Azure disaster recovery using Site Recovery Manager](#)

### Important requirements

- For Site Recovery Manager, an Azure VMware Solution SDDC must be already available and configured. VMware Cloud Activation™ services can help to set up the SDDC if needed.
- Please read the [Site Recovery Manager Release Notes](#), and [Azure VMware Solution instructions](#) 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.