VMware Cloud Activation Add-On Services

At a glance

VMware Cloud Activation Add-On Services allow you to extend the activities provided by VMware Cloud Activation Essentials, Standard, and Advanced Services.

Key benefits

- Continue to leverage VMware experts during your cloud journey
- Free IT staff to work on business-critical activities
- Minimize disruption to existing resources and operations
- Enable your IT team through knowledge transfer

SKUs

Azure VMware® Solution
PS-AVS-ACT-ADD-C

Google Cloud VMware® Engine
PS-GCVE-ACT-ADD-C

Oracle Cloud VMware® Solution
PS-OCVS-ACT-ADD-C

VMware Cloud™ on AWS
PS-VMC-ACT-ADD-C

VMware Cloud™ on Dell EMC
PS-VMC-D-ACT-ADD-C

Service overview

VMware Cloud Activation™ Add-On Services extend activities related to VMware Cloud Activation Essentials, VMware Cloud Activation Standard, and VMware Cloud Activation Advanced Services. These add-on services help your team to continue to leverage VMware experts during your cloud journey. They also enable your team through knowledge transfer of best practices and information resources.

Workstreams options

These services allow you to choose only one (1) of the following workstreams:

- Workstream 1: Discovery and dependency mapping for up to one hundred (100) VMs
- Workstream 2: Migration of up to one hundred (100) VMs
- Workstream 3: Disaster Recovery (DR) solution configuration for up to hundred (100) VMs
- Workstream 4: Application security with VMware NSX® Distributed Firewall™ for up to ten (10) VMs
- Workstream 5: Network extension for migration or DR for one (1) SDDC
- Workstream 6: Configuration and testing of VMware Ransomware Recovery™ for VMware Cloud DR™ for up to (100) VMs

All workstreams require VMware vSphere® on-premises and/or VMware Cloud™ 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).

Workstream 1: Discovery and dependency mapping for up to one hundred (100) VMs

VMware will collect available asset data to analyze and map dependencies between VMs and recommend a high-level strategy, including advantages and disadvantages of selected migration or DR tools, bandwidth needed, and methods to be used.

VMware will conduct validation and reconciliation workshops/meetings based on the discovery findings with Customer.

Discovery activities require the use of VMware Aria Operations™ for Networks, and we recommended to start collecting data 2 weeks prior to the engagement start.

This workstream applies to the following cloud infrastructure:

- Azure VMware Solution
- Google Cloud VMware Engine
- Oracle Cloud VMware Solution
- VMware Cloud on AWS
- VMware Cloud on Dell EMC

Workstream 2: Migration of up to one hundred (100) VMs

VMware will create a migration plan including bundling and scheduling migration events, perform the migration in waves, and do a validation with the Customer to ensure the migration is accurate and complete.

Having a discovery and dependency mapping previously done is strongly recommended to effectively perform this workstream.

This workstream applies to the following cloud infrastructure:

- Azure VMware Solution
- Google Cloud VMware Engine
- Oracle Cloud VMware Solution
- VMware Cloud on AWS
- VMware Cloud on Dell EMC

Workstream 3: DR solution configuration for up to hundred (100) VMs

VMware will create DR plans including bundling VMs in protection groups, defining a replication frequency, and performing DR tests with Customer to verify that RTO and RPO match Customer business needs.

This workstream applies to the following cloud infrastructure:

- Azure VMware Solution using VMware Site Recovery Manager™
- Google Cloud VMware Engine using VMware Site Recovery Manager
- VMware Cloud on AWS using VMware Cloud Disaster Recovery™ or VMware Site Recovery™
- VMware Cloud on Dell EMC using VMware Site Recovery

Workstream 4: Application security with NSX Distributed Firewall for up to ten (10) VMs

VMware will provide a repeatable methodology for securing applications within the cloud infrastructure, leveraging the security policy framework with the NSX

Distributed Firewall for up to two (2) applications consisting of up to ten (10) VMs.

An initial workshop will establish the principles and build the knowledge for discovering and securing applications using firewall rules. Following the workshop, VMware will demonstrate requirements gathering through application or technical-lead interviews, data analysis and policy creation for an initial nominated application. VMware will supervise the Customer in configuring the remaining application or VMs in scope.

For this workstream it is strongly recommended to have VMware Aria Operations™ for Networks already collecting data at the source 2 weeks prior to the engagement start.

This workstream applies to the following cloud infrastructure:

- Azure VMware Solution
- Google Cloud VMware Engine
- VMware Cloud on AWS
- VMware Cloud on Dell EMC

Workstream 5: Network extension for migration or DR for one (1) SDDC

VMware will provide a series of workshops and guidelines for extending networking connectivity from on-premises to the cloud SDDC or between two (2) SDDCs.

An initial workshop will establish the requirements and the specific use-cases that need to be addressed, specifically for workload migrations or DR and testing. Following the workshop, VMware will demonstrate the implementation of the specific extension leveraging VMware software components (i.e., VMware HCX®, NSX L2/L3 VPNs or VMware Transit Connect™) and will provide a high-level design of the network extension use-case discussed.

This workstream applies to the following cloud infrastructure:

- Azure VMware Solution
- Google Cloud VMware Engine
- VMware Cloud on AWS
- VMware Cloud on Dell EMC

Workstream 6: Configuration and testing of VMware Ransomware Recovery for up to hundred (100) VMs

VMware Ransomware Recovery builds upon the rich set of foundational capabilities that VMware Cloud Disaster Recovery already provides to protect from disasters. The service will perform the configuration of VMware Ransomware Recovery features for the existing protection groups and will validate additional functionality provided with guided recovery workflow to identify the recovery point candidates and streamline the recovery operations.

This workstream applies only to the following cloud product:

- VMware Cloud on AWS using VMware Cloud Disaster Recovery™

Note: For all workstreams, please check the VMware Requirements and Product Interoperability Matrix links in the Appendix.

Service delivery description

Service activities will be entirely delivered remotely by VMware Professional Services as offshore resources. Due to the nature of some on-premises components and security aspects VMware requires Customer to join virtual sessions and engage their infrastructure, network, and security teams when appropriate to execute required actions (e.g., 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.

Project scope

The scope of services delivered is dependent on which workstream is chosen:

- Workstream 1: Discovery and dependency mapping
- Workstream 2: Migration
- Workstream 3: DR solution configuration
- Workstream 4: Application security with NSX Distributed Firewall
- Workstream 5: Network extension for migration or DR
- Workstream 6: Configuration and testing of VMware Ransomware Recovery

The scope of activities is defined in the following tables grouped under the specific workstream.

Workstream 1: Discovery and dependency mapping

Discovery and dependency mapping activities are shown in the following table.

VMware Aria Operations for Networks		
Specification	Parameters	Description
VMware product required		A VMware Aria Operations for Networks subscription through http://cloud.vmware.com. Customer must provide access user account if Customer subscription is used.
VMware vCenter® instances	Up to one (1)	vCenter instances on-premises used during the application discovery process.

Applications	Up to twenty (20)	Unique application instances discovered and mapped, with an average of five (5) VMs for each app. complexity will affect the number.
Number of VMs	Up to one hundred (100)	Maximum number of VMs that will be analyzed. Complexity will affect the number.

Workstream 2: Migration

Migration activities are shown in the following table.

Virtual machine migration with VMware HCX		
Specification	Parameters	Description
Preliminary activities		Review of the discovered list of virtual machines planned for migration to the new SDDC.
On-premises Layer 2 networks extended	Up to one (1)	On-premises Layer 2 networks to extend with VMware HCX.
Virtual machines included in migration	Up to one hundred (100)	This is the total number of virtual machines in scope for this migration effort; only those that will fit into two (2) migration waves will be included.
Configure migration waves	Up to two (2)	Configure workload migrations in VMware HCX with proper resource selections for the target site. This includes monitoring and management of workload replication to ensure synchronization prior to the migration wave.
Run migration wave	Up to two (2)	During the scheduled migration window, the VMware Consultant will operate the VMware HCX console and facilitate the customer validation activities.

Workstream 3: DR solution configuration

VM protection activities are shown in the following table depending on the specific VMware solution used:

VMware Cloud Disaster Recovery or VMware Site Recovery Manager		
Specification	Parameters	Description
Preliminary activities		Review of the customer's provided list of workloads planned to be protected for DR the new SDDC.
Virtual machines included	Up to one hundred (100)	This is the total number of virtual machines in scope for DR Protection.
Protection groups	Up to seven (7)	Number of protection group(s) configured.
Recovery/DR plans	Up to two (2)	Number of recovery or DR plan(s) configured.
Recovery plan testing and cleanup	Up to two (2)	The test and cleanup for a recovery plan consisting of no more than five (5) VMs with each VM no larger than 200GB.

Workstream 4: Application security with NSX Distributed Firewall

Application security activities are shown in the following table.

VMware NSX Distributed Firewall		
Specification	Parameters	Description
Preliminary activities		Review of the customer's environment, verification of VMware NSX-T™ configuration and VMware Operations for Network collected data.
Number of infrastructure service policies	Up to five (5)	Security rules used for core and foundation services (e.g., NTP, Active Directory, DNS, etc.).
Number of High-level policies	Up to one (1)	Security policy that segments between broadly defined object groups (e.g. tenants, business units, environments).
Number of applications to be secured	Up to two (2)	Target applications identified for micro-segmentation, with each application comprised of up to five (5) virtual machines.

Workstream 5: Network extension for migration or DR

Network segment extension activities are shown in the following table.

Network Extension		
Specification	Parameters	Description
Preliminary activities		Discuss Customer use-case for network connectivity extension between source and target VMware SDDC through discovery workshops.
Workshops	Up to five (5) workshops	Review of Customer existing network architecture and configuration details. Identifying technical requirements, technical component, traffic flow specifications, network address translation and security rules specification for the following topologies: VMware HCX L2, L2 VPN, L3 VPN and vendor-specific connectivity. Determine routing policies and the application flow over the extended network between SDDCs
Source SDDC	Up to one (1)	Source VMware SDDC of the network extension, i.e. an existing on-premises VMware SDDC.
Destination SDDC	Up to one (1)	Target VMware Cloud SDDC for the network extension;
Network segments extended	Up to five (5)	Number of networking segments that will be extended, i.e., using VMware HCX L2 extension;

Workstream 6: Configuration and testing of VMware Ransomware Recovery

VM protection activities are shown in the following table:

VMware Cloud Disaster Recovery™		
Specification	Parameters	Description
Preliminary activities		Review of the customer's VMware Cloud Disaster Recovery environment and identification of workloads planned to be protected for Ransomware.

Virtual machines included	Up to one hundred (100)	This is the total number of virtual machines in scope for ransomware recovery.
Protection groups	Up to seven (7)	Number of protection group(s) configured.
Ransomware Recovery plans	Up to two (2)	Number of ransomware plan(s) configured.
Ransomware recovery plan testing and cleanup	Up to two (2)	The test and cleanup for a recovery plan consisting of validation the workflow to identify valid recovery point of no more than five (5) VMs with each VM no larger than 200GB.

Estimated schedule

VMware estimates that the duration for each individual workstream described will not exceed 3 weeks. VMware Professional Services 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).

Out of scope

The following are out of scope items for the defined project workstreams:

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

- Creation of user roles and groups
- Creation of local accounts
- Configuration of additional LDAP/Active Directory sources
- vCenter content library creation, OS images creation/copy/sync
- Creation of networking segments, VPNs, and additional firewall rules not included in the specific service scope
- Third-party vendor networking solutions (i.e., AWS Direct Connect, Microsoft ExpressRoute, Google Cloud Interconnect) configuration and troubleshooting
- Design or configuration of interconnectivity between different SDDCs or other native cloud services

VMware HCX

- Creation of additional network extensions or stretched networks not included in the specific service scope
- Deployment of additional target or source endpoints
- Deployment and configuration of Enterprise features like OSAM, MON, RAV or mobility groups
- Mixed cloud infrastructure for Initial target and initial source

VMware disaster recovery solutions

- Configuration or troubleshooting of on-premises networking and firewall components
- 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
- Mixed cloud infrastructure for protected and recovery sites

Ransomware protection and recovery

- VMware will not provide any specific tools to simulate ransomware attacks

Workload migration

- Pre- and post-application validation
- Backup/restore of virtual machines
- Multi-instances databases and/or part of database clusters will not be migrated
- Virtual machines with raw device mappings (RDM)
- Virtual machines with SCSI bus sharing cannot be migrated.

- NSX security tags and configurations related to the virtual machine will not be migrated.
- Virtual machine (with) snapshots
- Migration of physical to virtual environments
- Migration of clustered virtual machines
- Migration of virtual machines other than vSphere as source and target
- Migration of firewall rules, network, and security appliances not specified in the current document

Application security

- Applications hosted on physical workloads or containers.

Network extension

- Activation, deployment, configuration or troubleshooting of physical networking devices
- Deployment, configuration and troubleshooting of third-party vendor networking solutions (i.e., AWS Direct Connect, Microsoft ExpressRoute, Google Cloud Interconnect)

Project activities

Phase 1: Initiate

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

This phase applies to all workstreams and will cover the following topics:

- Project business drivers, workstream scope identification, 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 project
- 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.

This phase applies to all workstreams, and the objectives 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
- Workstream-specific kickoff presentation

Phase 3: Build

VMware will assess, implement, and provide knowledge transfer for all workstreams. VMware will also perform additional implementation activities for workstream 1, workstream 2, and workstream 3.

3.1 Assess (for all workstreams)

VMware leads the Customer project team in a series of workshops and data collection activities to collect Customer-specific data and determine gaps between the current state and target state.

Deliverables

- Technology discovery summary report

3.2 Implement (for all workstreams and individual workstreams)

VMware will perform implementation activities that will be carried out for all workstreams, as well as additional implementation activities specific to workstream 1, workstream 2, and workstream 3.

3.2.1 For all workstreams

For all workstreams, VMware implements the solution according to the VMware solution specification.

Deliverables

- Solution specification workbook
- Solution verification workbook
- Solution high-level design

3.2.2 For workstream 1: Discovery and dependency analysis

These activities apply to Customer's that have selected workstream 1.

3.2.2.1 Discovery

This workstream 1 subphase includes the following activities:

- Collect available asset data including asset dependencies
- Provide high-level strategy recommendations, including advantages and disadvantages of selected migration or DR tools, bandwidth needed, and methods
- Conduct data collection interviews and workshops, per infrastructure owner and application owner based on the discovery findings.
- Conduct validation and reconciliation workshops/meetings based on the discovery findings with Customer
- Provide inventory list of in scope servers
- Complete discovery validation and subphase milestones

Deliverables include:

- Infrastructure discovery workbook

3.2.2.2 Dependency analysis

This workstream 1 subphase includes the following activities:

- Conduct workshops to review bundling strategy criteria
- Analyze dependencies among assets: applications, servers, and key Infrastructure components
- Finalize asset bundles and event schedule including event dates based on bundle and Customer calendar constraints
- Develop master migration or disaster recovery event workbook and review draft runbook
- Identify risks and prepare a mitigation plan
- Complete dependency analysis and subphase milestones

Deliverables include:

- Migration or DR runbook
- Workload bundling report

3.2.3 For workstream 2: Migration

The following activities apply to Customer's that have selected workstream 2:

- Conduct dry-run migration event and task validation
- Validate standard operating procedure and migration runbook
- Perform any required migration runbook adjustments and complete pre-migration event preparation
- Migrate in-scope virtual machines
- Follow up standard operating procedure and migration runbook validation

- Complete Migration phase milestone completion

Deliverables include:

- Migration runbook
- Workload bundling report

3.2.4 For workstream 3: DR solution configuration

The following activities apply to Customer's that have selected workstream 3:

- Review and validation of the VMs to be protected
- Creation of protection group(s)
- Creation of recovery plan(s)
- Testing activities for the recovery plan(s)

Deliverables include:

- Configuration workbook

3.2.5 For workstream 6: Configuration and testing of VMware Ransomware Recovery

The following activities apply to Customer's that have selected workstream 6:

- Review and validation of the VMs to be protected for ransomware
- Activation of VMware Ransomware Recovery
- Testing activities for the ransomware recovery plan(s)
- Knowledge transfer about identification of valid recovery point and operations streamlines

Deliverables include:

- Configuration workbook

3.3 Knowledge transfer (for all workstreams)

VMware conducts knowledge transfer sessions covering the implementation, and operational considerations relating to the scope of the project.

Deliverables:

- Adoption guide document
- Knowledge transfer workshop presentation
- Up to four (4) hours of knowledge transfer sessions

Phase 4: Close

VMware conducts a closure meeting of up to four (4) hours with the Customer covering project status, reviewing completions, next steps and how to engage with VMware support.

Learn more

Visit vmware.com/services.

Terms and conditions

All VMware service engagements are governed by the VMware General Terms and Professional Services Exhibit on the VMware ONE Contract Center. If you are located in the United States, the VMware contracting entity for the service will be VMware, Inc. If you are outside the United States, the VMware contracting entity will be VMware International Limited.

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.

Appendix

The following Customer stakeholders are required to participate during the delivery of project activities:

- VMware operations team leads
- Application operations leads
- Security policy team leads
- Enterprise architect
- Infrastructure architect
- Network operations team leads
- Network architecture team leads

Requirements

To deliver the service accordingly to the expected timeline we require the following:

- Virtual machines must be running hardware version 9 or higher
- Virtual machines must have VMware tools installed
- Each virtual machine overall allocated disk size should not exceed more than 250 GB
- Distributed vSwitch must be in use for VMware Aria Operations for Networks and networks that need to be extended with VMware HCX
- The availability of the NTP service is critical to system operations
- Migration potential throughput can vary depending on bandwidth available for migrations, latency, available CPU/MEM/IOPS, and disk read speed. For more information about how to determine bandwidth requirements, see Bandwidth Requirements for vSphere Replication

Please verify product requirements and interoperability with the following:

- VMware Products interoperability matrix
- System Requirements for VMware HCX
- Software Version Requirements for VMware HCX
- VMware Cloud on AWS documentation
- VMware Cloud on Dell EMC documentation
- KB about VMware Cloud on Dell EMC End of Sales and End of Support
- Azure VMware solution documentation
- Google Cloud VMware Engine documentation
- Oracle Cloud VMware Solution documentation
- VMware Cloud Disaster Recovery documentation
- VMware Site Recovery Manager documentation
- VMware Site Recovery for VMware Cloud on AWS documentation
- VMware NSX Distributed firewall