Service Overview

Rackspace Managed VMware Cloud on AWS

VMware Cloud™ on AWS

Table of contents

Overview

VMware Cloud™ on AWS brings VMware enterprise-class Software Defined Data Center (SDDC) software to the AWS Cloud. This enables users to run production applications across private, public and hybrid cloud environments based on VMware vSphere®, with optimized access to AWS services.

VMware Cloud on AWS integrates VMware vCenter Server® management with VMware flagship compute, storage and network virtualization products, including VMware vSphere, VMware vSAN™, and VMware NSX®. This integration optimizes them to run on elastic, bare-metal AWS infrastructure with the same architecture and operational experience on premises and in the cloud. This provides IT teams with instant business value via the AWS and VMware hybrid cloud experience.

Rackspace Managed VMware Cloud on AWS is the ideal solution for customers looking for a simplified path to a hybrid-cloud through VMware Cloud on AWS. World-class account management and operations, including cross-platform billing, flexible payment options, proactive monitoring, market-leading SLAs and 24x7x365 support from a single partner delivers a unified and seamless experience. A unique Center of Excellence, developed in collaboration with VMware, delivers best-in-class VMware and AWS expertise to help you avoid integration challenges for an accelerated time to value to hybrid-cloud. And to optimize total cost of ownership in VMware Cloud on AWS and the AWS Cloud Platforms, you have access to a choice of comprehensive services and guidance to assist across architecture, migration and cloud transformation strategies.

Regional Availibility

As of November 2018, Rackspace Managed VMware Cloud on AWS is available in the following AWS Regions: U.S. West (Oregon), U.S. East (N. Virginia), EU (London), EU (Frankfurt), and Asia Pacific (Sydney). Rackspace will continue to work with VMware to make additional AWS Regions available as they come online. Please contact a Rackspace representative for the current list of supported regions.

Service Level Management

Rackspace offers 24x7x365 support for Managed VMware Cloud on AWS. Rackspace is one of VMware's largest global Cloud Provider Program partners with elevated access to technical specialists for the rapid resolution of unexpected software-related issues within the VMware stack.

VMware-Certified Professionals (VCPs) at Rackspace assist in the architecture, deployment, configuration and troubleshooting of the VMware Cloud on AWS environments. Rackspace will provision and configure the VMware Cloud on AWS SDDC in the available AWS region of your choosing along with any add-on services, then monitor your SDDC availability and capacity and provide support and assistance for SDDC configuration and troubleshooting.

Rackspace Managed VMware Cloud on AWS manages and supports the SDDC infrastructure. VMs or other virtual systems deployed, configured or created by you within the VMware Cloud on the AWS environment do not qualify for Rackspace managed services unless specifically enabled by an add-on service. Services for VMs such as OS or application monitoring, OS patching, antivirus and backups are your responsibility, unless you have purchased an add-on that provides that service.

Features

Enterprise-Grade Capabilities

- Leverage predictable, high-performance compute, storage and networking delivered by vSphere, vSAN and NSX running on next-gen Nitro system-based Amazon EC2 elastic, bare-metal infrastructure.
- Ensure application uptime through capabilities built directly into the service, such as vSphere HA, DRS, auto-host remediation and Stretched Clusters for zero-RPO infrastructure availability.
- Enable automatic scaling and load balancing of environments with Elastic DRS.
- Extend the value of your existing enterprise apps with high-bandwidth, low-latency access to AWS services.

Simple and Consistent Operations

- Create operational consistency across on-premises infrastructure and VMware Cloud on AWS. Organizations can continue to leverage existing application ecosystems, including familiar VMware management tools and APIs and integration with third-party tools validated to work with VMware Cloud on AWS.
- Get a single inventory view of both on-premises and VMware Cloud on AWS resources using vCenter Server technology.
- Focus on your apps while infrastructure patches and upgrades are managed for you.

Flexible Consumption and Investment Protection

- Align costs to your business needs with flexible consumption options and investment protection.
- Consume on-demand hourly, or take advantage of one-year and three-year reserved models for deeper discounts.
- Flexible payment options are available for subscriptions
- Add or remove hosts in minutes, or let Elastic DRS to do it automatically based on optimal utilization.

AWS Account And Fanatical Support For AWS Services

VMware Cloud on AWS is running directly on AWS elastic bare metal infrastructure, which provides high bandwidth, low latency connectivity to AWS services. Virtual machine workloads can access public API endpoints for AWS services such as AWS Lambda, Amazon Simple Queue Service (SQS), Amazon S3 and Elastic Load Balancing, as well as private resources in your Amazon VPC such as Amazon EC2, and data and analytics services such as Amazon RDS, Amazon DynamoDB, Amazon Kinesis and Amazon Redshift. The solution is designed to access AWS services while keeping all the traffic within the AWS network.

Whether or not you plan to integrate your SDDC workloads with AWS services, in order to use VMware Cloud on AWS, an AWS account is required. If you do not have an AWS account, you must establish one prior to being able to use Managed VMware Cloud on AWS. Prior to provisioning an SDDC, you will need to provide Rackspace with your AWS account so it can be linked to your VMware Cloud on AWS SDDC. This establishes the Identity and Access Management (IAM) policies in your AWS account, enabling communication between resources provisioned in your AWS account and your SDDC. AWS services consumed through your AWS account will be billed by AWS separately from your Managed VMware Cloud on AWS services and billing.

If you would like assistance with procuring and managing your AWS account, as well as guidance and support for utilizing AWS services, Rackspace Fanatical Support® for AWS is the answer. As a Premier Consulting Partner, Rackspace provides customized cloud service offerings to meet specific needs – giving you the flexibility to change or grow your cloud services as your AWS needs change, and increasing value by delivering the most-needed services and support. This includes architecture help, access to the expertise you need to solve your problems, security assistance, 24x7 management, cost governance and many other value-added services – all backed by AWS certified engineers and architects.

By combining Managed VMware Cloud on AWS with Fanatical Support for AWS services, you get:

- A Rackspace managed and supported AWS account to link with your Managed VMware Cloud on AWS environment
- Comprehensive cross-platform support across VMware Cloud on AWS and AWS services
- Guidance and support for migration of workloads to native AWS services
- Single vendor support and billing across VMware Cloud on AWS and AWS platforms
- Access to additional managed services and service blocks for AWS such as Architect & Deploy and Manage & Operate

You can find more information about Rackspace Fanatical Support for AWS in the Service Overview: https://manage.rackspace.com/aws/docs/product-guide/_downloads/service_overview_service_blocks.pdf.

You are not required to use Fanatical Support for AWS services to use Rackspace Managed VMware Cloud on AWS services. You can provide or obtain an AWS account directly from AWS and Rackspace will link that account to your VMware Cloud on AWS SDDC. In this case, Rackspace will have no visibility or access to AWS services in your AWS account and will not be able to provide support or specific guidance for those AWS services, and will be limited to providing support only for your Managed VMware Cloud on AWS environment.

Spheres Of Support

Rackspace is a Managed Service Provider for your VMware Cloud on AWS services. There are three parties involved in supporting your Rackspace Managed VMware Cloud on AWS environment, specifically:

- You – the customer (including any in-house IT resources)
- Rackspace – our VMware-certified support experts provide front end support, configuration assistance, and escalations to VMware
- VMware – Maintain SDDC software and infrastructure and backend services

The following table describes the service level activities associated with Managed VMware Cloud on AWS and the roles Rackspace and the Customer will have in each activity.

R – Responsible: party which performs an activity or does the work.

A – Accountable: party which is ultimately accountable completion of the activity.

C – Consulted: party which needs to or can provide feedback and contribute to the activity.

I – Informed: party which is kept up-to-date on the progress of the activity.

Managed VMware Cloud on AWS Service Level Activities

Service Level Activities	Rackspace	Customer	VMware
Account Management and Tooling			
Provide named Service Delivery Manager (SDM) resource	R, A	C, I	
Standard account reporting	R, A	C, I	
Identify opportunities for cost and performance optimization	R, A	C, I	
Provide opinions and best practices around account architecture, security and resiliency	R, A	C, I	
Discovery			
Understand business objectives and current challenges	R, A	C, I	
Schedule and conduct deep-dive discovery session	R, A	C, I	
Understand systems SLAs, RTO, PPO requirements	R, A	C, I	
Design/Architecture			
Define architecture options to be considered	R, A	C, I	
Agree on high-level design (HLD) architecture	C, I	R, A	
Generate high-level application/logical diagrams for proposed architecture(s)	R, A	C, I	
Generate detailed infrastructure schematics for proposed architecture(s)	R, A	C, I	
Create solution design document	R, A	C, I	
Design for high availability and security-first approach	R, A	C, I	
Design for sizing, scalability and performance	R, A	C, I	
SDDC Implementation			
Provisioning of SDDC infrastructure (network, storage, compute) in selected AWS region	R, A	C, I	
Configuration of vSphere virtual networking	R, A	C, I	
Configuration of NSX virtual networking and security	R, A	C, I	
Configure and test WAN connectivity for management VPN	R, A	C, I	
Create 1- or 3-year subscriptions	R, A	R, A	
Provide all required VMware SDDC licensing	I	I	R, A
User acceptance testing (UAT) and sign off environment deployment	C, I	C, I	
Implementation of ongoing change management for infrastructure components	R, A	C, I	
Add/Remove SDDC Cluster hosts on request	R, I	A, C	

Service Level Activities	Rackspace	Customer	VMware
Usage Measuring and Billing			
Measure and report on-demand host, hourly usage and metered usage charges	I	I	R, A
Monthly billing based on usage reports	R, A	C, I	
AWS Account and Optional Support			
Provide and manage linked AWS account with Fanatical Support for AWS as per Rackspace Service Relationships	R, A	C, I	
Provide and manage linked AWS account without Fanatical Support for AWS	I	R, A	
Support of AWS services with Fanatical Support for AWS as per Rackspace Service Relationships	R, A	C, I	
Support of AWS services without Fanatical Support for AWS	I	R, A	
Virtual Machine Support			
Provision and Manage Virtual Machines	C, I	R, A	
Manage and support VM guest Operating Systems	C, I	R, A	
Provide and ensure guest OS licensing compliance	C, I	R, A	
Monitoring			
Deployment and management of Rackspace standard monitoring services	R, A	C, I	
Ticketing/Alerting			
24x7x365 access to Fanatical Support for Rackspace standard monitoring services, including initial responses, escalations and troubleshooting of incidents within Rackspace response time, SLA guarantees	R, A	C, I	
Ongoing definition, management and maintenance of Rackspace's standard monitoring, platform, including the definition of alert triggers, thresholds and remediation instructions, initial response, escalation and troubleshooting	R, A	C, I	
SDDC Maintenance			
Installation/configuration of all VMware infrastructure-level updates and patching	I	I	R, A
Notification of Planned Maintenance to Rackspace	C, I		R, A
Notification of Planned Maintenance to Customer	R, A	C, I	
Backups			
Backup and restore of Management infrastructure including: vCenter Server, NSX Manager, NSX Controller and VMware NSX® Edge	C, I	I	R, A
Backup and restore of customer VMs and data	I	R, A	

Roles and Permissions

In a cloud SDDC, Rackspace and VMware perform numerous administrative tasks for you. This includes, but is not limited to, managing the lifecycle of the cloud SDDC software stack (deployment, configuration, patching, etc.), configuring the AWS infrastructure, and adding/removing hosts and networks during failure scenarios or cluster-scaling operations. Because the service is doing all of this for you, a cloud administrator in the SDDC requires fewer privileges than an administrator user on an on-premises data center.

vCenter Permissions and Roles

To better maintain the separation between the service and the customer, VMware Cloud on AWS introduces two new roles to the traditional vCenter user model: CloudAdmin and CloudGlobalAdmin. These new roles and associated privileges ensure that the Cloud SDDC infrastructure is configured in a prescriptive deployment architecture and the customer cloud administrators cannot adversely reconfigure the management component or appliances. With this model, the customer cloud administrator has full control over their workloads while having a read-only view of management workloads and infrastructure.

- CloudAdmin Role: The CloudAdmin role has the necessary privileges for you to create and manage workloads on your SDDC. However, you cannot access or configure certain management components that are supported and managed by VMware, such as hosts, clusters and management virtual machines.
- CloudGlobalAdmin Role: The CloudGlobalAdmin role is associated with global privileges and allows you to perform only certain global tasks like create and manage Content Library objects.

A new vCenter user group called CloudAdminGroup will also be created and given the privileges associated with both roles.

The CloudAdmin and CloudGlobalAdmin roles are assigned against different inventory objects as follows:

CloudAdmin Role

- Workload Datastore
- Compute Resource Pool
- Customer Networks
- Workloads Folder
- Templates Folder

CloudGlobalAdmin Role

- vCenter Root & Tree

For a detailed chart of all of the privileges mapped to these two roles, you can review the Privileges Reference for CloudAdmin and CloudGlobalAdmin on VMware documentation website.

Compatibility

Managed VMware Cloud on AWS might not be compatible with all Rackspace products and services. Contact your Rackspace support specialist for detailed information about whether any specific Rackspace product is compatible with your Managed VMware Cloud on AWS environment.

Managed VMware Cloud on AWS Compatibility with Third-Party Products

You can access VMware Cloud on AWS by using various VMware services APIs. You can use any third-party management, orchestration or other tool that is compatible with these APIs. In this case, the functionality of any such tool is limited by the Managed VMware Cloud on AWS features and capabilities as described in this service guide. You will need to ensure that the VMware services API versions of your environment are compatible with the third-party tools that you want to use.

Managed VMware Cloud on AWS Compatibility When Elevated Permissions are Needed

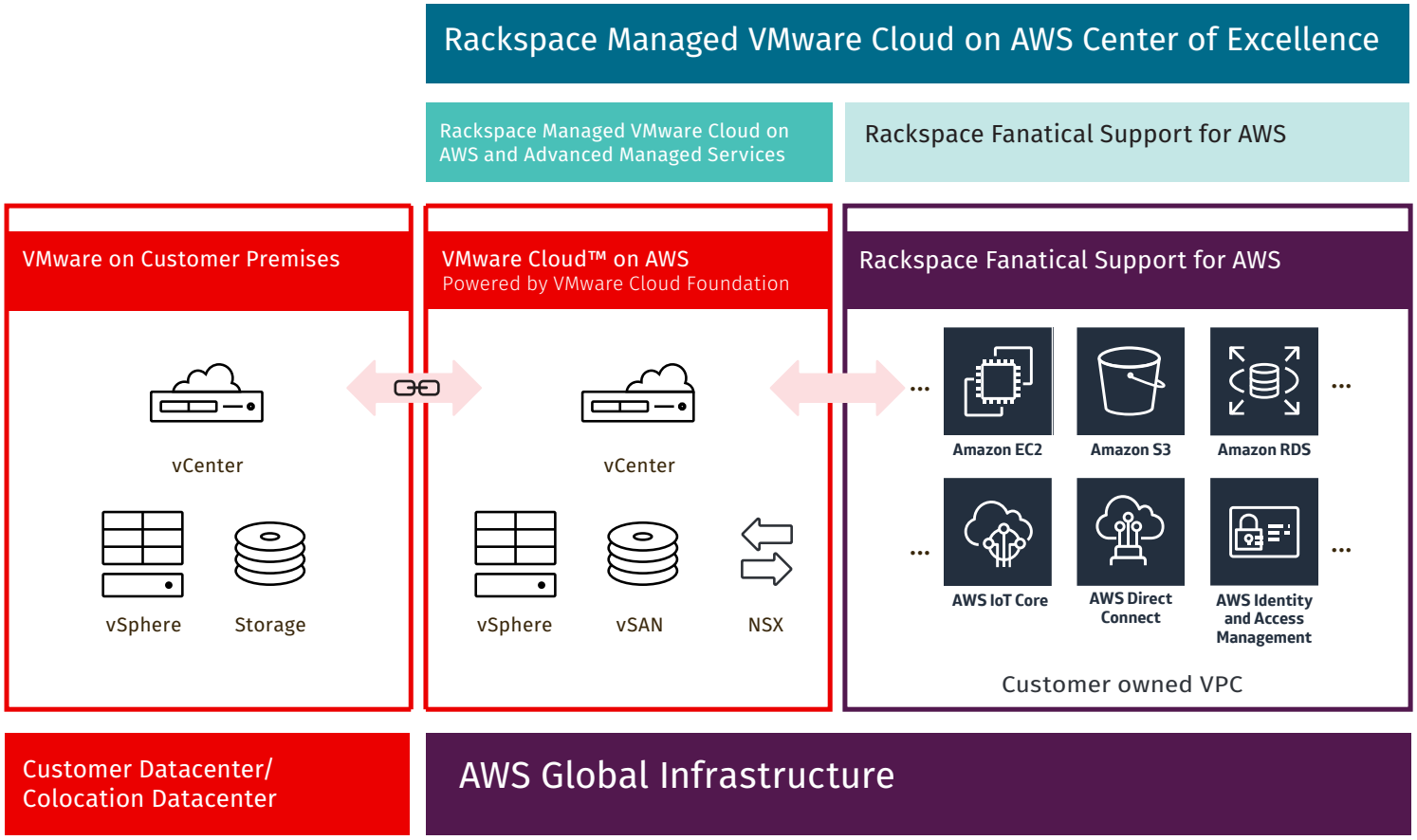
In some cases, existing role permissions provided by VMware or Rackspace do not allow a custom or third-party tool to function. Contact the Rackspace account team to determine if role permission adjustments are possible.

Managed VMware Cloud on AWS Authentication Methods

Managed VMware Cloud on AWS customers have two choices for vCenter authentication. When your private cloud is being built, you have the option to use either a Rackspace-provided directory service or your own Active Directory service.

Rackspace support still authenticates to your Managed VMware Cloud on AWS cloud with the Rackspace-hosted directory service. Your directory service is added as an additional authentication source. You must also indicate the groups and roles to be assigned in vCenter from the vCenter roles.

Architecture



VMware Cloud on AWS, powered by VMware Cloud Foundation™, integrates VMware flagship compute, storage and network virtualization products – VMware vSphere, VMware vSAN, and VMware NSX – along with VMware vCenter Server management. It optimizes them to run on elastic, bare-metal AWS infrastructure. With the same architecture and operational experience on-premises and in the cloud, IT teams can now get instant business value via the AWS and VMware hybrid cloud experience.

Compute – VMware vSphere

The VMware Cloud on AWS minimum cluster configuration contains 1.5TB of memory and three hosts. Each host is configured with 512GB of memory and contains dual CPU sockets that are populated by a custom-built Intel® Xeon® Processor E5-2686 v4 CPU package. Each socket contains 18 cores running at 2.3GHz, resulting in a physical cluster core count of 108. VMware Cloud on AWS uses a single, fixed host configuration; the option to add components to the host configuration is not offered at this time. However, the scale-out model enables expansion to up to 16 hosts, resulting in 576 CPU cores and 8TB of memory. VMware vSphere® Distributed Resource SchedulerTM (vSphere DRS) is enabled by default but can be disabled if desired.

Storage – VMware vSAN

The SDDC cluster includes a vSAN all-flash array. Each host is equipped with eight NVMe devices and a total of 10TB of raw capacity, not including the cache capacity of the vSAN datastore, for the VMs to consume. Within a VMware Cloud on AWS three-host cluster configuration, 30TB of raw capacity, comprising all 24 encrypted NVMe devices, is available for the VMs to consume. If the cluster is expanded to 16 hosts, 160TB of raw capacity is available for the VMs to consume, along with 128 encrypted NVMe devices. For all cluster configurations, the usable VM storage capacity depends on the per-VM storage policy. Each host contains eight NVMe devices distributed across two vSAN disk groups. Within a disk group, the write-caching tier leverages one NVMe device with 1.7TB of storage; the storage capacity tier leverages the other three NVMe devices with a combined 5.1TB of storage. Although default storage policy configuration settings are in place, you can configure your own storage policies to provide the appropriate protection level against host and component failure. The default storage policy setting for fault tolerance is RAID 1, but you can select RAID 5 or RAID 6 instead, depending on the number of hosts in the cluster.

Networking – VMware NSX

NSX is a key ingredient of VMware Cloud on AWS. It is not only optimized, along with vSphere, to work in the AWS environment, but it also provides all VM networking in VMware Cloud on AWS. NSX connects the VMware ESXi host and the abstract Amazon Virtual Private Cloud (VPC) networks. It enables ease of management by providing logical networks to VMs and automatically connecting new hosts to logical and VMkernel networks as clusters are scaled out. NSX is delivered using an "as-a-service" cloud model.

To provide connectivity to VMware Cloud on AWS, two gateways are created. The management edge gateway (MGW) utilizes VMware NSX® EdgeTM to enable you to connect to the vCenter Server instance. You can configure firewall rules, an IPsec VPN, and DNS for the management gateway. The customer gateway (CGW) utilizes an NSX Edge instance and a distributed logical router (DLR) to enable ingress and egress of VM network traffic. You can configure firewall rules, inbound NAT, VPN connections, DNS, and public IP addresses for their compute gateway. The initial customer configuration supports a single customer gateway. By default, all NSX Edge instances are large sized and are monitored for utilization. A default logical network is DHCP enabled and is provisioned with source NAT to provide outbound Internet connectivity. Note that some of these configurations may have to be done for you by Rackspace.

Support

Ticketing Process

One of the primary ways that you can interact with Rackspace is by creating a ticket in the Rackspace Customer Portal (https://racker.my.rackspace.com/portal/home). Once logged in, click the "Tickets" button from the menu to create a new ticket or view an existing ticket. Our automated systems will also create tickets for events on your account that require either your attention or the attention of a Rackspace employee. You can also call the 24x7x365 Support Team at any time.

Incident Response: All customer-submitted requests are automatically categorized as Standard requests. Rackspace will respond to your support requests in the following time frames:

Standard: If your site is functioning within acceptable parameters, but you require assistance in loading software or have a help desk–type question, we will respond to your request within four hours.

Urgent: If your server or site is accessible but in a reduced state (timeouts or slow response), we will respond to your support request within one hour.

Emergency: If you cannot access your server or site from the public internet, we will respond within 15 minutes.

Note: For requests that require an urgent or emergency classification, please call the 24x7x365 support line directly.

Source: Managed VMware Cloud on AWS Product Terms at https://www.rackspace.com/information/legal/managed-vmc-aws

Phone Support

You can call the 24x7x365 Support team to speak live to a Racker, and we'll be happy to assist.: 1-800-961-2888.

VMware Escalations

Rackspace is the sole point of contact for supporting your VMware Cloud on AWS environments. If VMware ever needs to be contacted, Rackspace will do so on your behalf.

Escalations may occur for the following scenarios:

- An issue that requires the involvement of a specific VMware Cloud on AWS product team to resolve
- Requests for clusters larger than 16 hosts
- An issue where multiple customers are impacted (VMware Cloud on AWS service outages)
- VMware Cloud on AWS availability SLA credit requests

Rackspace has direct access to VMware Support teams for emergency or critical escalations.

Response Time SLA

Support shall be available on a continuous (year-round, all day) basis. Upon receiving a support request, Rackspace shall designate each request according to the following severity categories.

Category	Definition	Example	Response Time
Emergency	Customer is unable to fulfil its business objectives.	You cannot access your Managed VMware Cloud on AWS environment from the public internet, or it is otherwise partially or wholly inoperable.	15 Minutes
Urgent	Customer's business objectives are impaired, but not completely obstructed.	Your Managed VMware Cloud on AWS environment is accessible but operating in a reduced state; such as slow API response.	1 Hour
Standard	Issue is non-critical or some anomalous behavior in Customer's VMware Cloud on AWS.	Your Managed VMware Cloud on AWS environment is generally functioning, but you have questions or need configuration assistance; also includes support call classified as incidents.	4 Hours

The above response times are applicable to all issues related to the Managed VMware Cloud on AWS platform and add-on services and are response times, not resolution times. Rackspace makes no guarantee regarding the time to resolve a support request.

Please refer to the below product terms for more information:

Managed VMware Cloud on AWS Product Terms at: https://www.rackspace.com/information/legal/managed-vmc-aws

Incident Management

Incident management refers to the management of incidents where restoration of services is the primary objective. Rackspace endeavors to restore normal service as quickly as possible when an incident occurs.

Rackspace will apply a consistent approach to all incidents, except where a specific approach has been previously agreed upon with you in accordance with your accounts runbook. Incidents can be initiated by named account contacts and you can expect the following from the Rackspace Incident Management process:

All incidents are logged in tickets accessible via the Rackspace Customer Portal at: https://racker .my .rackspace .com/portal/home. Rackspace support teams will investigate the incident in accordance with your service level, once logged.

Priority for tickets entered manually via the Customer Portal is initially set to "Standard." Should you desire an escalation of priority, please phone your Rackspace support team or your assigned Service Delivery Manager. Incidents logged with a specific priority will not be changed to another priority without the agreement of all parties involved.

Prior to investigation, Rackspace support will carefully review instructions on your account (documented via the account runbook).

Rackspace will collaborate with you as well as with any third parties you nominate as technical contacts on your account to resolve the incident.

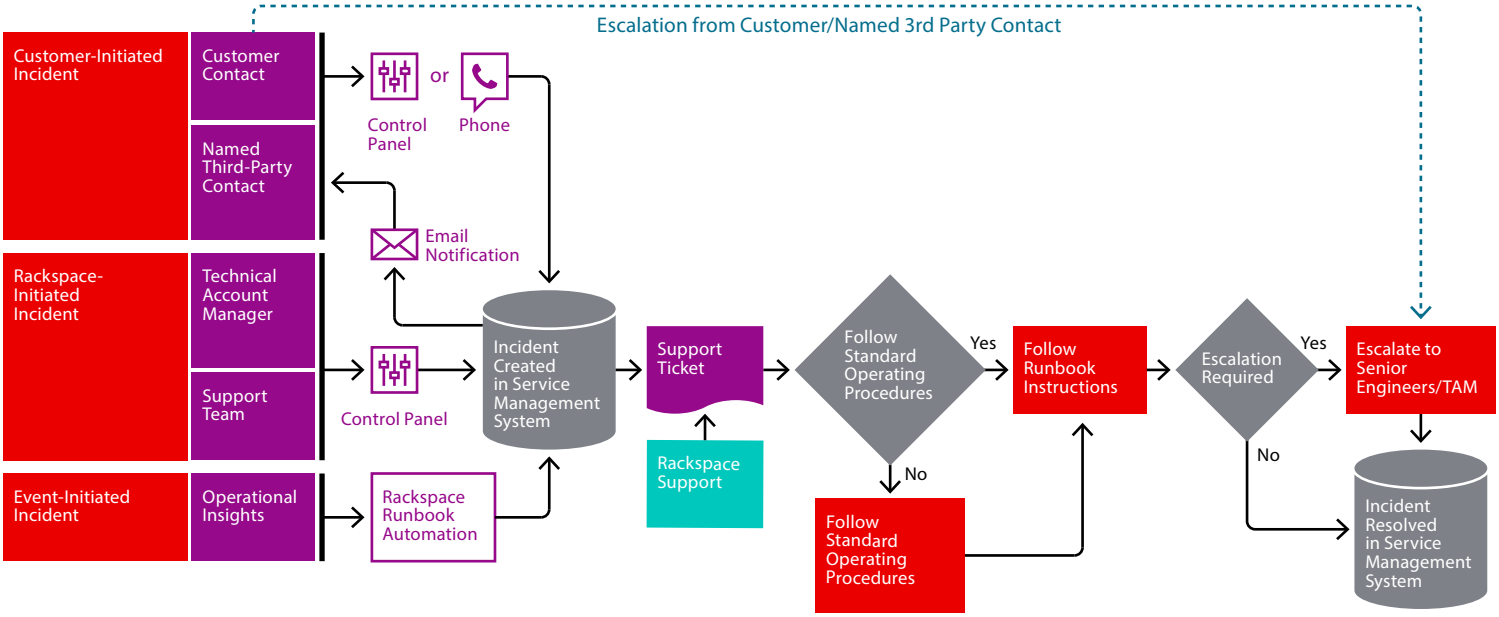
At all times, you will have visibility into which support engineer is working on the incident.

Rackspace support teams will communicate regularly with you throughout the incident, detailing their findings and any actions taken.

If a support engineer is unable resolve an incident, he or she may escalate the incident at any time until resolution is achieved. This escalation may be hierarchical (to a more-senior engineer or the Service Delivery Manager) or functional (involving specialized technical expertise from other functional groups or VMware).

The action required to resolve an incident will vary depending on investigative findings. In some cases, a proposed solution may be complex or cause additional disruptive impact to your VMware environments. In these cases, the incident will be handled as a change through the Rackspace change management process, and you will be consulted to determine the time window during which the solution or change may be implemented. Alternately, you may be required to take action to resolve the incident, which will be communicated should such a need occur.

An incident is deemed closed when you confirm that it is resolved. This is achieved through the incident ticket being set to "Solved" status. You may also phone into the 24x7x365 support line to discuss a change and request a ticket be created.



Change Management

Change management includes a standardized set of procedures that enables Rackspace to deliver efficient and prompt handling of all changes in an organized manner to help ensure minimum impact on the services.

- Your Rackspace Service Delivery Manager will be available to work with you on all operational, technical and commercial changes to the environment.
- All changes will be managed through the Rackspace ticketing systems. This supports long-term tracking of all information and the optimum delivery of services through the various lifecycle processes of deployment, change management, incident management, etc.
- Rackspace will raise a ticket accessible via the Rackspace Customer Portal for changes that are owned or initiated by Rackspace. Conversely, you can raise a ticket for situations where Rackspace support is required for any changes owned and initiated by your business. You may also call the 24x7x365 support line to discuss a change and request a ticket be created.
- Rackspace will organize the support engineers with specific domain expertise to manage the change as scheduled, keeping you fully informed on progress.

Patching

VMware will periodically patch or upgrade the various SDDC components in your Managed VMware Cloud on AWS environment. These services will be patched or upgraded as needed and to address critical vulnerabilities and maintain the health and availability of the VMware Cloud on AWS service.

Rackspace will receive notice from VMware of scheduled maintenance and will try to obtain your consent before patching or upgrading the environment to ensure that actions are performed at a convenient time for you. This process will not require any scheduled downtime for virtual systems deployed by you in your environment, but it might temporarily impact the availability of the various user interfaces and APIs of the VMware Cloud on AWS services. The patching or upgrade of hosts might affect the performance of virtual systems deployed by you in your environment if the patch or upgrade requires a host to be restarted. Performance should return to normal when host patching or upgrading is complete.

Backups

VMware Cloud on AWS management components are backed up by VMware as part of the VMware Cloud on AWS service. Contact Rackspace if you believe it is necessary to restore management service components from backups, and Rackspace with work with you and with VMware to address the issue. You are responsible for backups of your virtual machines and other data. Backups for virtual machines that you create are not provided by Rackspace.

Add-On Services

HCX Migration Assistance

Transitioning from an existing environment to VMware Cloud on AWS requires specific expertise and resources skilled in technology transformation, migration planning and risk mitigation. VMware Hybrid Cloud Extension (HCX) is included with all VMware Cloud on AWS SDDC targets. For additional fees, Rackspace will setup your HCX environment, and can optionally own the process of migrating your virtual machines to your VMware Cloud on AWS SDDC. Please engage your sales representative for further information regarding pricing and timelines.

Appendix

Frequently Asked Questions

General

Q: How do I access VMware Cloud on AWS?

A: You can access VMware Cloud on AWS through a VPN connection. Rackspace will help you configure access to your Management and Compute networks.

Q: In which AWS Regions can I deploy Managed VMware Cloud on AWS?

A: As of November 2018 Rackspace Managed VMware Cloud on AWS is available in the following AWS Regions: U.S. West (Oregon), U.S. East (N. Virginia), EU (London), EU (Frankfurt), and Asia Pacific (Sydney). Rackspace will continue to work with VMware to make additional AWS Regions available as they come online. Please contact a Rackspace representative for the current list of supported regions.

Q: Are backups included with Managed VMware Cloud on AWS?

A: VMware Cloud on AWS environments are backed up by VMware. Contact Rackspace if you believe it is necessary to restore management service components from backup. Backups for virtual machines that you create are not provided and are not currently available from Rackspace, but are under consideration as an add-on for the future.

Q: Does Rackspace manage or support my virtual machines running on VMware Cloud on AWS?

A: Management and support of virtual machines and guest operating systems is not included in Managed VMware Cloud on AWS. These services are not currently available for this platform, but are under consideration as an add-on for the future.

Q: How can I migrate virtual machines to my VMware Cloud on AWS SDDC?

A: You can migrate data to Rackspace by using a number of VMware and third-party solutions. Rackspace can provide services to configure migration solutions such as VMware Hybrid Cloud Extension (HCX) or vCenter Hybrid Linked Mode, and can own the process of migrating for additional fees. For more information about migrating to VMware Cloud on AWS, contact Rackspace.

Licensing

Q: Is VMware licensing included in VMware Cloud on AWS?

A: Yes, the Managed VMware Cloud on AWS service includes the required VMware licensing for all SDDC components: vSphere, vSAN and NSX.

Q: Can I use my existing VMware licenses on VMware Cloud on AWS?

A: You cannot apply your existing VMware licenses to your VMware Cloud on AWS environment, but you can leverage existing VMware software investments to obtain additional discounts from 10 percent to 25 percent for your VMware Cloud on AWS subscriptions through the VMware Hybrid Loyalty Discount Program. Contact Rackspace for more details.

Q: Is VM guest operating system licensing included in Managed VMware Cloud on AWS?

A: No, licensing for your VM guest operating systems is not provided by Rackspace or by VMware. You are responsible for ensuring all VM guest operating systems are properly licenses.

Architectural

Q: Are VMware Cloud on AWS environments deployed in a high availability (HA) configuration?

A: Yes, VMware Cloud on AWS environments are deployed in an HA configuration.

Q: Is there a limit to the number of VMs per environment?

A: Rackspace does not impose a limit on VMs per environment. We can provide recommendations for best practices to maintain optimal performance.

Q: Can I access the vCenter API?

A: Yes. You can access the vCenter and vSphere APIs, subject to permissions restrictions on a user account.

Q: What cluster sizes are supported?

A: Supported cluster size is from three to 16 hosts. Clusters up to 32 hosts are possible but require an exception approval. Contact Rackspace for details.

Q: Can I add or remove hosts to my Managed VMware Cloud on AWS environment?

A: Yes, it is easy to add or remove hosts from a SDDC cluster as long as you do not go below minimum configuration or above maximum configuration limits. Rackspace will need to complete this action for you. Please contact Rackspace support.

Q: Can I manage vCenter plug-ins and add my own third-party plug-ins?

A: This will depend on the vCenter permissions required by the particular plug-in. See the vCenter Permissions and Roles section for more details about the customer role permissions provided. Validate the third-party plug-in is supported with VMware Cloud on AWS. Rackspace may be able to assist you in registering the plug-in with your vCenter server.

Q: Are storage RDMs supported?

A: Yes, you can get support for raw device mappings (RDMs) by opening a support ticket with our storage and virtualization team.

Integration

Q: What other VMware products are supported?

A: VMware has validated compatibility with many other VMware products like VMware vRealize® OperationsTM and VMware vRealize® AutomationTM. Visit the VMware website for the latest compatibility matrix: https://cloud.vmware.com/vmc-aws/solutions#vmware-solutions

Q: Is Rackspace RackConnect Global supported with Managed VMware Cloud on AWS?

A: Yes, Rackspace RackConnect® Global can be used to connect your Managed VMware Cloud on AWS environment to solutions such as Rackspace Private Cloud Powered by VMware (RPC-V) in Rackspace datacenters. For RPC-V deployments in customer's datacenters or third-party datacenters, please speak with your sales representative.

Monitoring

Q: How are Managed VMware Cloud on AWS components monitored?

A: The management infrastructure is monitored by using the following combination of tools:

- Both VMware and Rackspace monitor aspects of your Managed VMware Cloud on AWS environment. VMware is responsible for the health and availability of VMware Cloud on AWS management components and infrastructure.
- Rackspace service monitors are created to ensure that web services associated with Managed VMware Cloud on AWS are available. If they become unavailable, the monitoring service alerts Rackspace virtualization engineers to investigate and resolve the issue, engaging VMware as needed.
- Rackspace monitoring services are configured to inspect vCenter alarms and alerts are sent to Rackspace virtualization engineers for alarms raised in vCenter. Rackspace also monitors utilization and available capacity of your SDDC clusters.

Q: Is monitoring provided for my VMs?

A: Rackspace does not provide monitoring for VMs on Managed VMware Cloud on AWS at this time. Rackspace may provide monitoring for VMs in the future through an optional add-on.

About Rackspace

At Rackspace, we accelerate the value of the cloud during every phase of digital transformation. By managing apps, data, security and multiple clouds, we are the best choice to help customers get to the cloud, innovate with new technologies and maximize their IT investments. As a recognized Gartner Magic Quadrant leader, we are uniquely positioned to close the gap between the complex reality of today and the promise of tomorrow. Passionate about customer success, we provide unbiased expertise, based on proven results, across all the leading technologies. And across every interaction worldwide, we deliver Fanatical Experience™ — the best customer service experience in the industry. Rackspace has been honored by Fortune, Forbes, Glassdoor and others as one of the best places to work.

Learn more at www.rackspace.com or call us at 1-800-961-2888.