# VMC on AWS PACSI Matrix

## Updated July 2019

Kevin Lees

Chief Technologist, IT Operations Transformation

July 2019

# Operationalizing VMware Cloud on AWS: PACSI Matrix

## Table of Contents

# Executive Summary

VMware Cloud on AWS provides a unified infrastructure framework that enables businesses to integrate their on-premise, VMware SDDC platform with AWS. It does so while providing a common operating environment in which existing tools and skillsets based on familiar VMware software can be leveraged. This is extremely powerful but comforting at the same time. That said, there are some operational differences between managing an on-premise VMware SDDC platform and VMware Cloud. To help address the differences and their impact on operational roles and responsibilities at the activity level, we've developed a VMware Cloud PACSI matrix.

While there are obvious differences when compared to physical data management, the main operational differences lie in what you can and can't do in vCenter when managing the SDDC environments you deploy in VMware Cloud. Administrators are accustomed to both seeing and modifying pretty much every aspect of the on-premise SDDC environment. In VMware Cloud, the Cloud Administrator role can still see essentially all of the same SDDC environment settings but is restricted in what they can modify. There are also some operational process responsibility differences. These differences are most pronounced in the following categories: SDDC Management, Compute Management, Storage Management, Network Management, and Security Management. The PACSI matrix also addresses role responsibilities for activities in other areas more specific to managing VMware Cloud, specifically: Organization Management, Workload Management, On-premise to VMware Cloud on AWS Connectivity Management, and VMware Cloud on AWS to AWS Access Management.

# Executive Summary

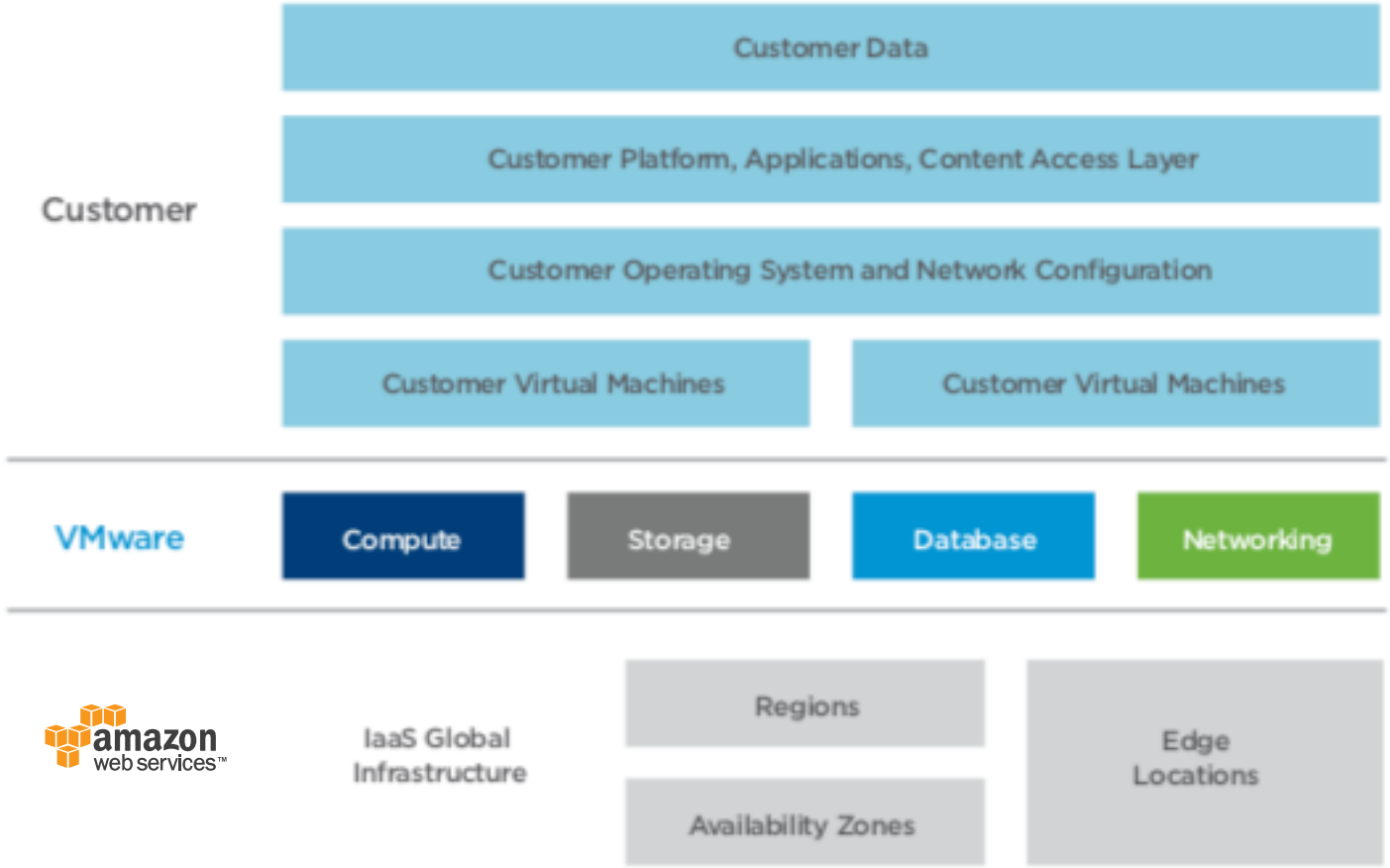
While differences with on-premise operational activities do exist, the consensus among those who are managing SDDC environments on VMware Cloud is that the biggest challenge is making the mindset shift to work within the constraints that exist when managing with vCenter. Once that mindset shift is accomplished, they find managing SDDC environments on VMware Cloud and working with the VMware team managing the underlying environment easy and seamless. Once they do, IT can fully leverage capabilities provided by their on-premise VMware SDDC to VMware Cloud integrated hybrid cloud and realize the benefits of having a common operating environment.

# PACSI

| | |
|---|---|
| Perform | The person/function carrying out the activity |
| Accountable | The person/function ultimately answerable for the correct and thorough completion of the deliverable or task, and often the one who delegates the work to the performer |
| Control | The person/function reviewing the result of the activity (other than the accountable). He or she has a right of veto; his or her advice is binding |
| Suggest | The person/function consulted to give advice based upon recognized expertise. The advice is non-binding. |
| Informed | The person/function who must be informed of the result of the activity. |

Reference: https://en.wikipedia.org/wiki/Responsibility_assignment_matrix - PACSI

# Scope




https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/products/cloud-services/vmware-cloud-services-on-aws-security-overview-white-paper.pdf

# Roles

AWS (CSP)

VMware (CSP)

Customer Cloud Admin (tenant vCenter)

Cloud Organization Owner

Cloud Organization Member

NSX Admin

NSX Cloud Auditor

Customer Workload Admin

# Categories

## Where are the biggest differences with on-premise?

Physical Datacenter Management

Organization Management

SDDC Management (vCenter)

- Compute Management
- Storage Management
- Network Management
- Security Management

Workload Management

On-premise to VMware Cloud on AWS Connectivity Management

VMware Cloud on AWS to AWS Access  Management

# Physical Datacenter Management

| VMware Cloud on AWS Operations PACSI<br>(**P**erform, **A**ccountable, **C**ontrol, **S**uggest, **I**nformed) | *AWS (CSP)* | *VMware (CSP)* | *Customer Cloud Admin (tenant vCenter)* | *Customer Cloud Global Admin (deprecated)* | *Cloud Organization Owner* | *Cloud Organization Member* | *NSX Admin* | *NSX Cloud Auditor* | *Customer Workload Administrator* |
|---|---|---|---|---|---|---|---|---|---|
| **Physical Datacenter Management** | | | | | | | | | |
| Operations for underlying physical infrastructure of the data center, across all regions and availability zones, as well as edge locations | P,A | | | | | | | | |
| Create and manage physical VMware on AWS network | P,A | | | | | | | | |

# Organization Management

| VMware Cloud on AWS Operations PACSI (Perform, Accountable, Control, Suggest, Informed) | AWS (CSP) | VMware (CSP) | Customer Cloud Admin (tenant vCenter) | Customer Cloud Global Admin (deprecated) | Cloud Organization Owner | Cloud Organization Member | NSX Admin | NSX Cloud Auditor | Customer Workload Administrator |
|---|---|---|---|---|---|---|---|---|---|
| **Organization Management** | | | | | | | | | |
| Apply subscriptions | | | | | P,A | P,S | | | |
| Invite users to organization | | | | | P,A,C | | | | |
| Assign permissions to users | | | | | P,A,C | | | | |
| Assign cloud services to users | | | | | P,A,C | | | | |
| Create SDDC | | I,S | | | P,A,C | P,S | | | |
| Add users to customer vCenter | | | P,A,C | | | | | | |
| Assign users to roles in customer vCenter | | | P,A,C | | | | | | |
| View and edit the default vCenter Single Sign-On password policy, lockout policy, and token policy | | | P,A,C | | | | | | |
| Manage vCenter users | | | P,A,C | | | | | | |

# SDDC Management (vCenter)

| VMware Cloud on AWS Operations PACSI (Perform, Accountable, Control, Suggest, Informed) | AWS (CSP) | VMware (CSP) | Customer Cloud Admin (tenant vCenter) | Customer Cloud Global Admin (deprecated) | Cloud Organization Owner | Cloud Organization Member | NSX Admin | NSX Cloud Auditor | Customer Workload Administrator |
|---|---|---|---|---|---|---|---|---|---|
| **SDDC Management (vCenter)** | | | | | | | | | |
| Patching and updating of customer on-premise SDDC components | | S | | | | | | | P,A |
| Creation, deletion, and maintenance of SDDC component (Cloud Organization Owner can assign delete restriction to Cloud Organization Members) | | I | | | P,A,C | P,A,C | | | |
| SDDC software component backup and restore | | P,A | I | | | | | | |
| SDDC software component disaster recovery | | P,A | I | | | | | | |
| Backup and restore of configurations created by the customer in the customer's SDDC, including virtual machines, Content Libraries, datastores, and port groups | | | | | | | | | P,A,C |
| Patching and updating of SDDC components comprising the VMC on AWS service offering ( *NOTE: customer can influence timing of upgrades, customer accountable for decision to upgrade or not) | | P | A,I,C* | | | | | | |
| Incident & Problem Management related to VMC on AWS service offering | | P,A | I | | | | | | |
| Change Management related to maintaining the health and availability of the VMC on AWS Service Offering | S | P,A,C | I | | | | | | |
| Notification of scheduled VMC on AWS Service Offering maintenance | | P,A | I | | | | | | |
| Change Management related to customer's SDDC environment | | P,A | I | | | | | | |
| Ensure sufficient capacity for customers in each data center | C | P,A | | | I | I | | | |
| Oversubscription settings for memory and compute resources in customer's SDDC | | | P,A,C | | | | | | S,I |
| Maintain adequate capacity of customer's SDDC environment in accordance with customer's regulations, compliance, and requirements | | | P,A,C | | | | | | |

# SDDC Management (vCenter): Compute Management

| VMware Cloud on AWS Operations PACSI (Perform, Accountable, Control, Suggest, Informed) | AWS (CSP) | VMware (CSP) | Customer Cloud Admin (tenant vCenter) | Customer Cloud Global Admin (deprecated) | Cloud Organization Owner | Cloud Organization Member | NSX Admin | NSX Cloud Auditor | Customer Workload Administrator |
|---|---|---|---|---|---|---|---|---|---|
| Request to add or remove host | | I | | | P,A,C,S | P,S,I | | | |
| Replace host (includes automatic re-balancing of workloads within cluster via DRS) | | P, A, C | I | | | | | | |
| Provision physical hosts | A | P,C,S | I | | | | | | |
| Physical host naming (IP Address-based host naming only) | | P, A, C | I | | I | I | | | I |
| View host settings | | P, A, C | P | | | | | | |
| Configure host | | P, A, C | I | | I | I | | | I |
| Patching host | | P, A, C | I | | I | I | | | I |
| Add, remove host drivers (VIB) | | P, A, C | | | | | | | |
| Add, remove host tags and customer attributes | | | P,A,C,S | | | | | | C |
| Add, remove clusters | | | | | P,A,C,S | P,C,S,I | | | I |
| Monitor cluster settings | | P,A,C | P,S | | P,C,S | | | | |
| Edit cluster settings | | P,A,C | | | | | | | |
| Add, remove cluster tags and custom attributes | | | P,A,C | | | | | | S,I |
| Add, remove compute child resource pools | | | P,A,C | | | | | | S,I |
| Edit compute child resource pool settings (Name, Shares, Reservations, Expandable Reservation, Limit) | | | P,A,C | | | | | | S,I |
| Add, remove compute resource pool tags and customer attributes | | | P,A,C | | | | | | S,I |

# SDDC Management (vCenter): Storage Management

| VMware Cloud on AWS Operations PACSI (Perform, Accountable, Control, Suggest, Informed) | AWS (CSP) | VMware (CSP) | Customer Cloud Admin (tenant vCenter) | Customer Cloud Global Admin (deprecated) | Cloud Organization Owner | Cloud Organization Member | NSX Admin | NSX Cloud Auditor | Customer Workload Administrator |
|---|---|---|---|---|---|---|---|---|---|
| **Storage Management** | | | | | | | | | |
| Request storage addition to vSAN datastores (via requesting additional host) | | I | I | I | P,A,C | P,C | | | |
| Monitor vSAN usage (NOTE: especially 70% vSAN capacity threshold to satisfy SLA) | | P,A,C | P,C | | P,C | P,C | | | |
| Create vSAN datastore | | P,A | | | | | | | |
| Create, edit storage policies | | | P,A,C | | | | | | I |
| Select default storage policy | | P | P,A,C | | | | | | |
| Turn on deduplication, compression, & data at rest encryption (on by default) | | P,A,C | I | | | | | | I |
| Change Key Encryption Key (KEK) via shallow re-key | | | P,A,C | | | | | | |
| vSAN re-balancing when host added or replaced in a cluster | | A,P | I | | | | | | |

# SDDC Management (vCenter): Network Management

| VMware Cloud on AWS Operations PACSI (Perform, Accountable, Control, Suggest, Informed) | AWS (CSP) | VMware (CSP) | Customer Cloud Admin (tenant vCenter) | Customer Cloud Global Admin (deprecated) | Cloud Organization Owner | Cloud Organization Member | NSX Admin | NSX Cloud Auditor | Customer Workload Administrator |
|---|---|---|---|---|---|---|---|---|---|
| **Network Management** | | | | | | | | | |
| Create, edit, remove logical networks | | | | | | | P,A,C | I | |
| View distributed virtual switch settings | | A | I | | I | I | P,C,S,I | I | I |
| Create, edit, remove distributed virtual port groups | | P,A,C | I | | I | I | I | I | I |
| Monitor virtual distributed virtual port groups | | | | | I | I | P,A,C | P,I | I |
| Create and apply traffic filtering rules to distributed virtual port groups | | | | | | | P,A,C,S | I | |
| Request public IP address | I | I | | | | | P,A,C | I | |
| Manage NAT | I | I | | | | | P,A,C | I | |

# SDDC Management (vCenter): Security Management

| VMware Cloud on AWS Operations PACSI (Perform, Accountable, Control, Suggest, Informed) | AWS (CSP) | VMware (CSP) | Customer Cloud Admin (tenant vCenter) | Customer Cloud Global Admin (deprecated) | Cloud Organization Owner | Cloud Organization Member | NSX Admin | NSX Cloud Auditor | Customer Workload Administrator |
|---|---|---|---|---|---|---|---|---|---|
| **Security Management** | | | | | | | | | |
| Physical infrastructure security, audit, and compliance | P,A,C,S | P,C,S,I | | | | | | | |
| SDDC software components and the IaaS infrastructure security, audit, and compliance | | P,A | I | | | | | | |
| Customer data security including locality, transport, disposal | P,A | P | | | S,I | | | | |
| Customer administrative console, virtual machine, applications, and content access | | | P,A,C | | | | | | S,I |
| Customer SDDC logical network(s) security | | | | | I | I | P,A | I | |
| Customer SDDC security monitoring | | | P,I | | P,A | P | P | I | |
| Manage gateway firewall rules | | | | | | | P,A | I | |
| Manage distributed firewall rules | | | | | | | P,A | I | |
| Customer SDDC audit and compliance | P,S,I | P,A | P,C,S | | P,C,S,I | P | P | P | |
| In-guest encryption and key management | | | | | | | | | P,A |
| Integrity of virtual machine images associated with SDDC software components and IaaS infrastructure | S,I | P,A,C | I | | I | | | | |
| Integrity customer's virtual machine images | | | P,A,C | | | | | | P,S,I |

# Workload Management

| VMware Cloud on AWS Operations PACSI (Perform, Accountable, Control, Suggest, Informed) | AWS (CSP) | VMware (CSP) | Customer Cloud Admin (tenant vCenter) | Customer Cloud Global Admin (deprecated) | Cloud Organization Owner | Cloud Organization Member | NSX Admin | NSX Cloud Auditor | Customer Workload Administrator |
|---|---|---|---|---|---|---|---|---|---|
| **Workload Management** | | | | | | | | | |
| Add VM templates, OVF, OVA, ISO images, scripts, and test files to customer SDDC | | | P,A,C | | | | | | P,C,I |
| Migrate virtual machines into and out of customer SDDC | | | P,A,C | | | | | | P,C,I |
| Virtual machine power actions | | | P,A,C | | | | | | P,C,I |
| Upgrade VMTools in Guest OS | | | P,A,C | | | | | | P,C,I |
| Create, delete, and manage snapshots | | | P,A,C | | | | | | P,C,I |
| Create, delete, and manage virtual machine clones | | | P,A,C | | | | | | P,C,I |
| Edit, Check compliance, and reapply VM storage policies to virtual machines | | | P,A,C | | | | | | P,C,I |
| Can schedule virtual machine compatibility upgrade | | | P,A,C | | | | | | P,C,I |
| Edit virtual machine settings | | | P,A,C | | | | | | P,C,I |
| Move virtual machine to vCenter folder | | | P,A,C | | | | | | P,C,I |
| Rename virtual machine | | | P,A,C | | | | | | P,C,I |
| Virtual machine backup and restore | | | P,A,C | | | | | | P,C,I |
| Patching and updating of all customer virtual machines in their SDDC environment | | | P,A,C | | | | | | P,C,I |
| Customer virtual machine disaster recovery | | | P,A,C | | I | | | | P,C,I |
| Incident & Problem Management related to Customer virtual machines | | | P,A,C | | I | | | | P,C,I |

# On-premise to VMware Cloud on AWS Connectivity Management

| VMware Cloud on AWS Operations PACSI (Perform, Accountable, Control, Suggest, Informed) | AWS (CSP) | VMware (CSP) | Customer Cloud Admin (tenant vCenter) | Customer Cloud Global Admin (deprecated) | Cloud Organization Owner | Cloud Organization Member | NSX Admin | NSX Cloud Auditor | Customer Workload Administrator |
|---|---|---|---|---|---|---|---|---|---|
| **On-premise to VMware Cloud on AWS Connectivity Management** | | | | | | | | | |
| Create, edit, remove, monitor on-premise to customer SDDC logical networks | | | P,A,C | | | | | | P,C |
| Configure DNS server configuration for a management or compute gateway | | | | | | | P,A,C | I | P,C |
| Enable or disable DNS configuration for a management or compute gateway | | | | | | | P,A,C | I | P,C |
| Modify NAT configuration for a management or compute gateway | | | | | | | P,A,C | I | P,C |
| Modify route and policy-based VPN configuration for a management or compute gateway | | | | | | | P,A,C | I | P,C |
| Configure firewall for a management or compute gateway | | | | | | | P,A,C | I | P,C |
| Modify SDDC L2 VPN configuration | | | | | | | P,A,C | I | P,C |
| Append firewall rules for a management or compute gateway | | | | | | | P,A,C | I | P,C |
| Update the specific NAT rule for a management or compute gateway | | | | | | | P,A,C | I | P,C |
| HCX appliances on-premises updates (*NOTE: Customer is accountable to keep HCX updated to N -1 or will become out of support) | | | | | | P,A*,C | I | | I |
| Modify the specified firewall rule for a management or compute gateway | | | | | | | P,A,C | I | P,C |

# VMware Cloud on AWS to AWS Access  Management

| VMware Cloud on AWS Operations PACSI<br>(**P**erform, **A**ccountable, **C**ontrol, **S**uggest, **I**nformed) | *AWS (CSP)* | *VMware (CSP)* | *Customer Cloud Admin (tenant vCenter)* | *Customer Cloud Global Admin (deprecated)* | *Cloud Organization Owner* | *Cloud Organization Member* | *NSX Admin* | *NSX Cloud Auditor* | *Customer Workload Administrator* |
|---|---|---|---|---|---|---|---|---|---|
| **VMware Cloud on AWS to AWS Access  Management** | | | | | | | | | |
| Enable access to AWS Services | S,I | | | | P,A,C | | | | S,I |
| Extend logical networking to access AWS services | S,I | | | | P,A,C | | | | S,I |

# Thank You