VMware Cloud Well-Architected Framework for VMware Cloud on AWS: Shared Responsibility Model

VMware Operations and Management

Table of contents

VMware Cloud Well-Architected Framework for VMware Cloud on AWS: Shared Responsibility Model
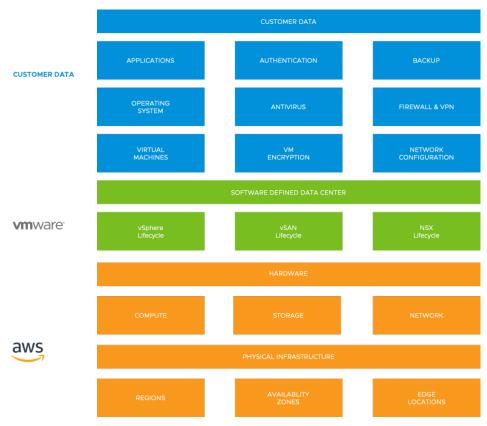
VMware Cloud Shared Responsibility

A shared responsibility model is common among the different VMware Cloud Infrastructure Service providers, which defines distinct roles and responsibilities between the VMware Cloud Infrastructure Services provider and an organization consuming the service**.**

Disclaimer: The intent of this document is to provide guidance and best practices for VMware Cloud Infrastructure Service providers regarding the shared responsibilities of the service.

VMware Cloud on AWS

VMware Cloud on AWS implements a shared responsibility model that defines distinct roles and responsibilities for the three parties involved in the offering: Customer, VMware, and Amazon Web Services.

CUSTOMER DATA

CUSTOMER DATA		
APPLICATIONS	AUTHENTICATION	BACKUP
OPERATING SYSTEM	ANTIVIRUS	FIREWALL & VPN
VIRTUAL MACHINES	VM ENCRYPTION	NETWORK CONFIGURATION

vmware®

SOFTWARE DEFINED DATA CENTER		
vSphere Lifecycle	vSAN Lifecycle	NSX Lifecycle

aws

HARDWARE		
COMPUTE	STORAGE	NETWORK

PHYSICAL INFRASTRUCTURE		
REGIONS	AVAILABLITY ZONES	EDGE LOCATIONS

Responsibilities

Customer Responsibility: Security in the Cloud

Customers are responsible for the deployment and ongoing configuration of their SDDC, virtual machines, and data that reside therein. In addition to determining the network firewall and VPN configuration, customers are responsible for managing virtual machines (including in guest security and encryption) and using VMware Cloud on AWS User Roles and Permissions along with vCenter Roles and Permissions to apply the appropriate controls for users.

VMware Responsibility: Security of the Cloud

VMware is responsible for protecting the software and systems that make up the VMware Cloud on AWS service. This software infrastructure is composed of the compute, storage, and networking software comprising the SDDC, along with the service consoles used to provision VMware Cloud on AWS.

AWS Responsibility: Security of the Infrastructure

AWS is responsible for the physical facilities, physical security, infrastructure, and hardware underlying the entire service. Details on the shared responsibility model employed by VMware Cloud on AWS can be found in the table below. You can see that a great deal of low-level operational work is handled by the VMware Cloud on AWS Site Reliability Engineering team leaving the customer to focus on managing their workloads.

Shared Responsibility Matrix

For a detailed description of the roles and responsibilities for VMware Cloud on AWS, please refer to the Service Description.

Entity	Responsibility/Activity
Customer	
VMware	
Amazon Web Services	

References

- Amazon Web Services: Overview of Security Processes

In the next section, learn about the different considerations for managing infrastructure and application services.