Shared Responsibility Model Overview

VMware Cloud on AWS

vmware®

Table of contents

Introduction

VMware Cloud on AWS (VMC) brings VMware's enterprise class software defined data center offering to the Amazon Web Services cloud, enabling customers to run any application across vSphere-based private, public, and hybrid cloud environments.

VMware Cloud on AWS has the following components:

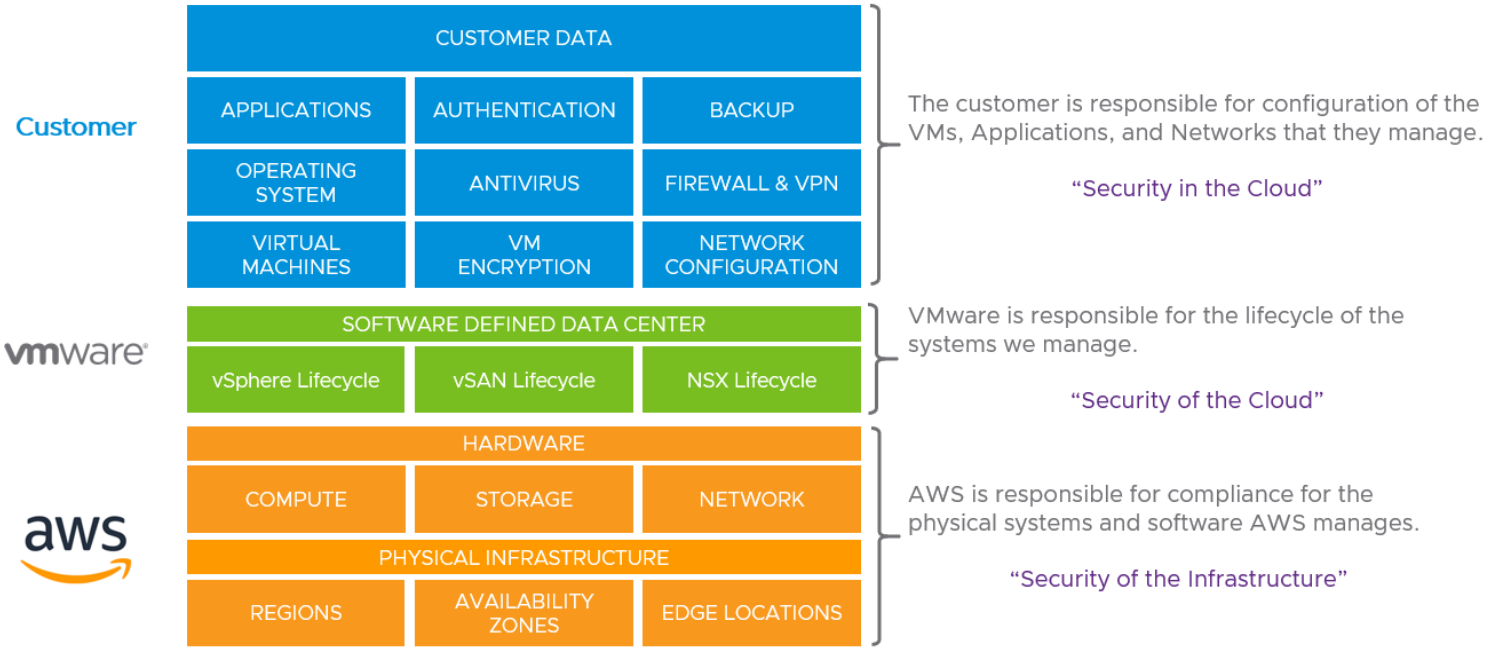
Software Defined Data Center ("SDDC") consisting of:

- VMware vSphere® running on elastic bare metal hosts deployed in AWS
- VMware vCenter Server® appliance
- VMware NSX® Data Center to power networking
- VMware vSAN aggregating host-based storage into a shared datastore
- VMware HCX® enabling app mobility and infrastructure hybridity
- Self-service provisioning of SDDCs, on demand, from vmc.vmware.com
- Maintenance, patching, and upgrades of the SDDC, performed by VMware

VMware has been offering this enterprise grade infrastructure as a service since 2017 and is delivering thousands of production workloads for customers 24x7x365.

Shared Responsibility Model

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



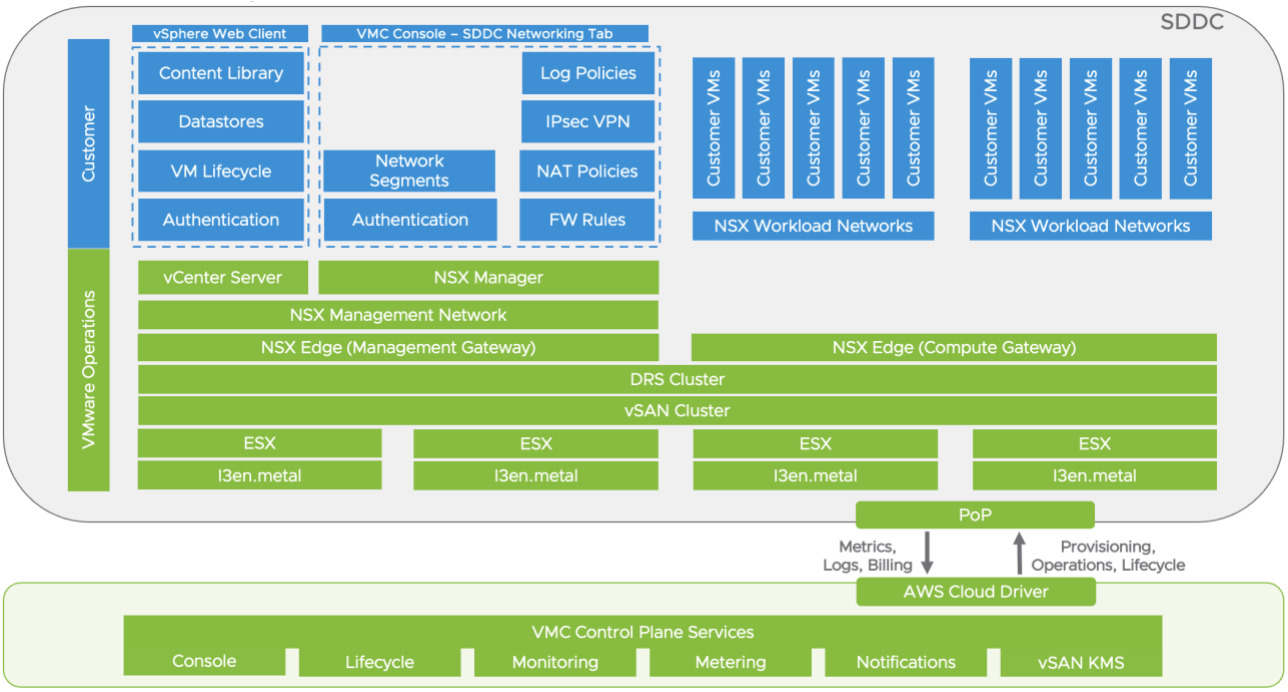
Customer responsibility "Security in the Cloud" – Customers are responsible for the deployment and ongoing configuration of their SDDC, virtual machines, and data that reside therein. In addition to determining the network firewall and VPN configuration, customers are responsible for managing virtual 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.

SDDC Inventory Responsibilities

The VMware Cloud on AWS Software Defined Data Center includes management inventory that is operated by VMware along with inventory that is operated by the customer. The diagram below color codes the SDDC inventory to help clarify the shared responsibility model with customer responsibilities represented in green and VMware responsibilities represented in dark blue.



Shared Responsibility Matrix

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.

Entity	Responsibility/Activity

Customer	• Deploying Software Defined Data Centers (SDDCs)
	  ○ Host Type (i3.metal, r5.metal, etc.)
	  ○ Host Count
	  ○ Connected AWS Account
	  ○ Management Network Range
	• Configuring SDDC Network & Security (NSX)
	  ○ Management Gateway Firewall
	  ○ Management Gateway IPsec VPN
	  ○ Compute Gateway Firewall
	  ○ Compute Gateway IPsec VPN
	  ○ Compute Gateway NAT
	  ○ Public IP Addresses
	  ○ Network Segments
	  ○ Distributed Firewall
	• Deploying Virtual Machines
	  ○ Installing Operating Systems
	  ○ Patching Operating Systems
	  ○ Installing Antivirus Software
	  ○ Installing Backup Software
	  ○ Installing Configuration Management Software
	• Migrating Virtual Machines
	  ○ Live vMotion
	  ○ Cold Migration
	  ○ Content Library Sync
	• Managing Virtual Machines
	  ○ Installing software
	  ○ Implementing backup solution
	  ○ Implementing in-guest encryption
	  ○ Implementing Antivirus solution
	• Managing Vulnerabilities
	  ○ Scanning and applying security patches to deployed virtual machines and applications

VMware	• SDDC Lifecyle
	  ○ ESXi patch and upgrade
	  ○ vCenter Server patch and upgrade
	  ○ NSX patch and upgrade
	  ○ vSAN patch and upgrade
	• SDDC Backup/Restore
	  ○ Backup and Restore vCenter Server
	  ○ Backup and Restore NSX Manager
	• SDDC Health
	  ○ Replace failed hosts
	  ○ Add hosts to maintain adequate “slack space”
	• SDDC Provisioning
	  ○ Operate vmc.vmware.com 24x7x365
	  ○ Manage “Shadow” VPC holding customer SDDC
	• Managing vulnerabilities

	○ Scanning and applying security patches to the standard VMware SDDC infrastructure components within the SDDC (e.g. NSX, vSAN, ESX, vCenter)
Amazon Web Services	• Physical Infrastructure ○ AWS Regions ○ AWS Availability Zones ○ Physical security of AWS facilities • Compute / Network / Storage ○ Rack and Power Bare Metal Hosts (ie i3.metal and i3en.metal) ○ Rack and Power Network Equipment

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

References

- VMware Cloud on AWS Getting Started Guide

  https://docs.vmware.com/en/VMware-Cloud-on-AWS/services/vmc-on-aws-getting-started.pdf

- VMware Cloud on AWS Service Description

  https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/support/vmw-cloud-aws-service-description.pdf

- VMware Cloud Services Security Overview

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

- Amazon Web Services: Introduction to AWS Security

  Introduction to AWS Security - AWS Whitepaper (amazon.com)

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 vmware.com.