Technical White Paper: **2023**

Shared Responsibility Model Overview

VMware Cloud on AWS Outposts

vmware®

Table of contents

Introduction 2
Shared responsibility model 3
SDDC inventory responsibility 4
Shared responsibility matrix 5
References 5

Introduction

VMware Cloud on AWS Outposts brings VMware enterprise class software defined data center offering to on-premises datacenter and edge locations. VMware Cloud on AWS Outposts provide simple, secure and scalable infrastructure that removes the friction of day-to-day tasks with cloud-like ease of use for on-premises workloads. It offers consistency between on-premises and public cloud environments.

VMware Cloud on AWS Outposts has the following components:

- VMware Software Defined Data Center ("SDDC") consisting of
  - VMware vSphere® ESXi running on AWS EC2 bare-metal server
  - VMware vCenter® Server Appliance
  - VMware NSX® Data Center for vSphere to power networking for the service
  - VMware vSAN™ aggregating host-based storage into a shared datastore
  - VMware HCX to enable app mobility and infrastructure hybridity
- AWS-supplied hardware – AWS EC2 bare-metal server, switches, racks, UPS, etc.
- Customer self-service provisioning of SDDCs through VMware's Cloud Portal
- SDDC maintenance, patching and upgrades, performed by VMware
- AWS hardware maintenance, patching and upgrades, performed by Amazon Web Services
- AWS-provided network to an AWS Region - used by VMware for remote management

Note: In addition to the above components, every rack also includes spare capacity, i.e., a spare host not configured as part of the running cluster. In the event of a hardware-related degradation, the spare node can be activated to replace an unhealthy host in the cluster. The impaired node can then be repaired remotely or swapped without affecting the application uptime.

Shared responsibility model

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

Customer	Customer data		
	Applications	Authentication	Backup
	Operation system	Antivirus	Firewall & VPN
	Virtual machines	Containers	Network (segments & virtual firewall)

The customer is responsible for compliance for the VMs, networks, and applications that they manage.

VMware operations	Software defined data center		
	vSphere lifecycle	vSAN lifecycle	NSX lifecycle
	Compute	Storage	Network (NSX-T overlay)

VMware is responsible for lifecycle management of the components comprising the SDDC.

AWS	Hardware	
	Physical infrastructure (rack, PDU, Switches, etc.)	

Amazon Web Services is responsible for the infrastructure.

Customer	Datacenter Power, cooling, physical security or facility	Edge Location Power, cooling, physical security or facility

Customer is responsible for the managing the datacenter facilities, power, and cooling. Refer to link at the end of the document.

Customer responsibility

Customers are responsible for the deployment and ongoing configuration of their SDDC, virtual machines, and data that reside therein. In addition to determining the data center facilities (power, cooling, etc.), network, firewall and uplink connections, customers are responsible for managing virtual machines and using VMware Cloud on AWS Outposts user roles and permissions along with vCenter roles and permissions to apply the appropriate controls for users. In addition, customers are responsible for the physical facilities including their temperature control and security. Customers are responsible for providing reliable internet-facing access at a minimum of 100Mbps.

VMware responsibility

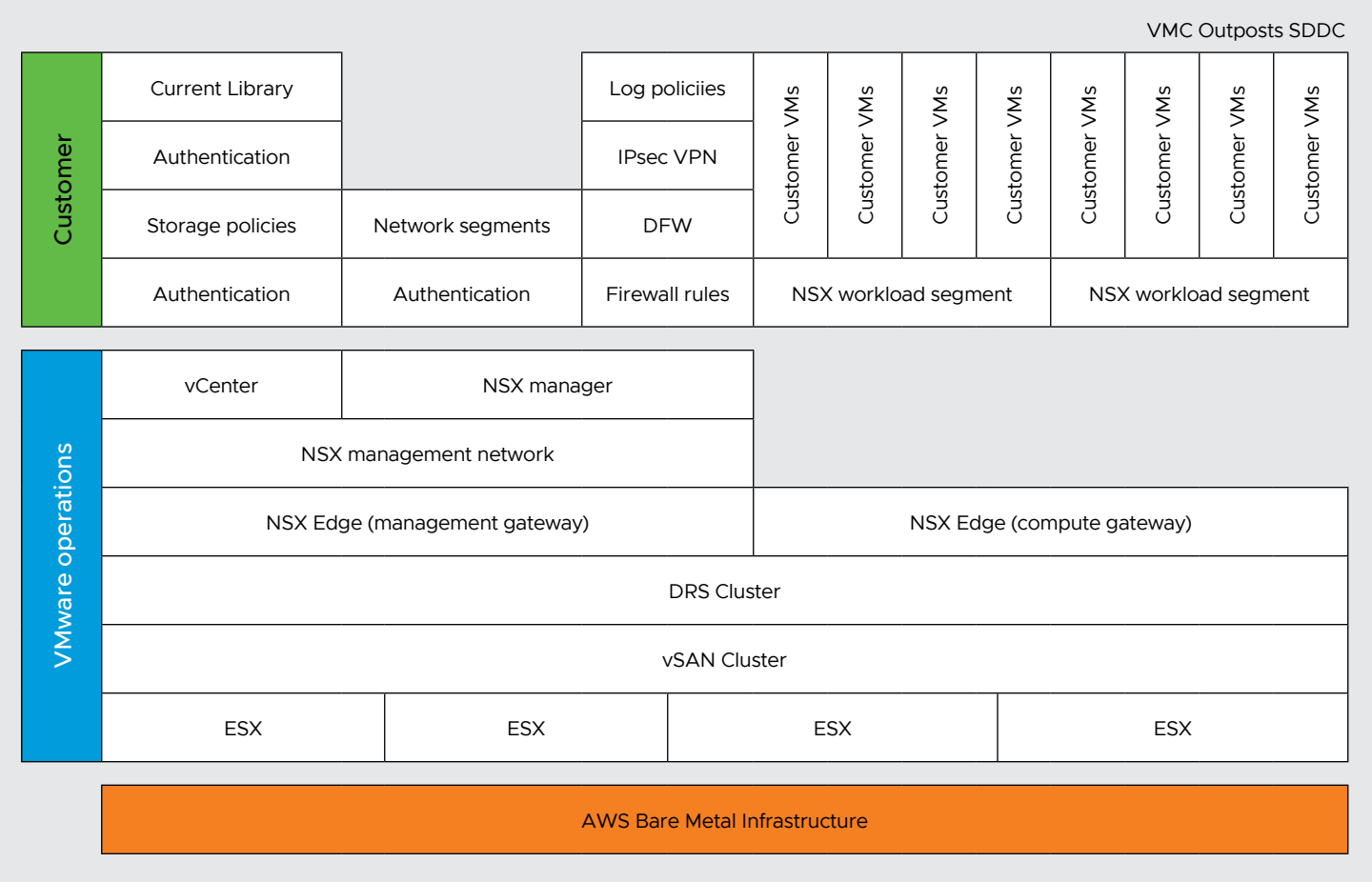
VMware is responsible for protecting the software and systems that make up the VMware Cloud on AWS Outposts service. This software infrastructure is composed of the compute, storage and networking software comprising the SDDC, along with the service consoles used to provision VMware Cloud on AWS Outposts.

Amazon Web Services responsibility

Amazon Web Services is responsible for providing and maintaining the physical infrastructure that includes rack, host hardware, networking gear and PDU.

SDDC inventory responsibility

The VMware Cloud on AWS Outposts 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 blue.



Shared responsibility matrix

Details on the shared responsibility model employed by VMware Cloud on AWS Outposts 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 Outposts Site Reliability Engineering team, giving customers the ability to focus on workload and policy management.

Entity	Responsibility/Activity
Customer	Deploying Outposts Rack • Manage physical network and connectivity to VMware Cloud on AWS Outposts network • Implement adequate HVAC systems and access controls within the rack location • Implement adequate power and controls to support VMware Cloud on AWS Outposts racks • Establish strict access control to physical location of VMware Cloud on AWS Outposts racks • Physical Infrastructure security, audit, and compliance under customer's responsibility Deploying Software Defined Data Centers (SDDCs) Host Type (i3en.metal) • Host Count • Connected AWS Account • Management Network Range Configuring SDDC Network and Security (NSX) • Management Gateway Firewall • Compute Gateway Firewall, IPsec VPN, NAT • 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

Entity	Responsibility/Activity
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 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) Security and Encryption • Deduplication, compression, and data-at-rest encryption • Encryption Key Management
AWS	Physical Infrastructure • AWS Regions • AWS Availability Zones Compute / Network / Storage • Rack and Bare Metal Hosts (i3en.metal) • Rack and Power Network Equipment • Customer data security including locality, transport, disposal while consuming native services

References

For additional resources for VMware Cloud on AWS Outposts, please refer to the Service Description and documentation linked below.

VMware Cloud on AWS Outposts Launchpad

VMware Cloud on AWS Outposts Service Description

Item No: 81042 Shared Responsibility Model Overview VMC on AWS Outposts White Paper 1/23